

ISS

CLI User Manual_Vol6

Copyright © 2010 Interface Masters Inc. All Rights Reserved. No part of this document may be reproduced, stored in a retrieval system or transmitted, in any form, or by any means, electronic or otherwise, including photocopying, reprinting, or recording, for any purpose, without the express written permission of Interface Masters.

Printed in _____

TRADEMARKS INTERFACE MASTERS and THE INTERFACE MASTERS LOGO are trademarks of Interface Masters Inc. in the U.S. and other countries. The use of any of these trademarks without Interface Masters prior written consent is strictly prohibited. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Interface Masters Inc. disclaims any proprietary interest in the trademarks and trade names other than its own.

DISCLAIMER The information in this book is provided “as is”, with no warranties whatsoever, including any warranty of merchantability, fitness for any particular purpose or any warranty otherwise arising out of any proposal, specification or sample. This document is provided for informational purposes only and should not be construed as a commitment on the part of Interface Masters. Information in this document is subject to change without notice.

REQUESTS For information or obtaining permission for use of material of this work, please submit a written request to: Corporate Marketing and Legal, Interface Masters on www.InterfaceMasters.com.

DOCUMENT No.: INTERFACE MASTERS: ISSCLlum_Vol6/20101001

Contents

CHAPTER 47:	IGMP SNOOPING	7
47.1	IP IGMP SNOOPING	10
47.2	IP IGMP SNOOPING PROXY-REPORTING	12
47.3	SNOOPING MULTICAST-FORWARDING-MODE	13
47.4	IP IGMP SNOOPING MROUTER-TIME-OUT	14
47.5	IP IGMP QUERIER-TIMEOUT	15
47.6	IP IGMP SNOOPING PORT-PURGE-INTERVAL	16
47.7	IP IGMP SNOOPING SOURCE-ONLY LEARNING AGE-TIMER	17
47.8	IP IGMP SNOOPING REPORT-SUPPRESSION INTERVAL	18
47.9	IP IGMP SNOOPING RETRY-COUNT	19
47.10	IP IGMP SNOOPING GROUP-QUERY-INTERVAL	20
47.11	IP IGMP SNOOPING REPORT-FORWARD	21
47.12	IP IGMP SNOOPING QUERY-FORWARD	22
47.13	IP IGMP SNOOPING VERSION	23
47.14	IP IGMP SNOOPING FAST-LEAVE	24
47.15	IP IGMP SNOOPING VLAN - IMMEDIATE LEAVE	25
47.16	IP IGMP SNOOPING QUERIER	26
47.17	IP IGMP SNOOPING QUERY-INTERVAL	27
47.18	IP IGMP SNOOPING STARTUP-QUERY-INTERVAL	28
47.19	IP IGMP SNOOPING STARTUP-QUERY-COUNT	29
47.20	IP IGMP SNOOPING OTHER-QUERIER-PRESENT-INTERVAL	30
47.21	IP IGMP SNOOPING MROUTER	31
47.22	IP IGMP SNOOPING VLAN MROUTER	32
47.23	SHUTDOWN SNOOPING	33
47.24	DEBUG IP IGMP SNOOPING	34
47.25	SNOOPING LEAVE-PROCESS CONFIG-LEVEL	36
47.26	IP IGMP SNOOPING ENHANCED-MODE	37
47.27	IP IGMP SNOOPING SPARSE-MODE	38
47.28	SNOOPING REPORT-PROCESS CONFIG-LEVEL	39
47.29	IP IGMP SNOOPING MULTICAST-VLAN	40
47.30	MVR	41
47.31	IP IGMP SNOOPING FILTER	42
47.32	IP IGMP SNOOPING BLOCKED-ROUTER	43
47.33	IP IGMP SNOOPING MULTICAST-VLAN PROFILE	44
47.34	IP IGMP SNOOPING LEAVEMODE	45
47.35	IP IGMP SNOOPING RATELIMIT	47
47.36	IP IGMP SNOOPING LIMIT	48
47.37	IP IGMP SNOOPING FILTER-PROFILEID	49
47.38	IP IGMP SNOOPING PROXY	50
47.39	IP IGMP SNOOPING MAX-RESPONSE-CODE	51
47.40	IP IGMP SNOOPING MROUTER-PORT -TIME-OUT	52
47.41	IP IGMP SNOOPING MROUTER-PORT-VERSION	54
47.42	SHOW IP IGMP SNOOPING MROUTER	55
47.43	SHOW IP IGMP SNOOPING MROUTER - REDUNDANCY	57
47.44	SHOW IP IGMP SNOOPING GLOBALS	58
47.45	SHOW IP IGMP SNOOPING	60
47.46	SHOW IP IGMP SNOOPING - REDUNDANCY	62
47.47	SHOW IP IGMP SNOOPING GROUPS	63
47.48	SHOW IP IGMP SNOOPING FORWARDING-DATABASE	65
47.49	SHOW IP IGMP SNOOPING FORWARDING-DATABASE - REDUNDANCY	67

	47.50 SHOW IP IGMP SNOOPING STATISTICS	68
	47.51 SHOW IP IGMP SNOOPING BLOCKED-ROUTER	71
	47.52 SHOW IP IGMP SNOOPING MULTICAST-RECEIVERS	72
	47.53 SHOW IP IGMP SNOOPING PORT-CFG	74
	47.54 SHOW IP IGMP SNOOPING MULTICAST-VLAN	78
CHAPTER 48:	MLD SNOOPING	81
	48.1 IPV6 MLD SNOOPING	83
	48.2 IPV6 MLD SNOOPING PROXY-REPORTING	84
	48.3 IPV6 MLD SNOOPING MROUTER-TIME-OUT	85
	48.4 IPV6 MLD SNOOPING PORT-PURGE-INTERVAL	86
	48.5 IPV6 MLD SNOOPING REPORT-SUPPRESSION-INTERVAL	87
	48.6 IPV6 MLD SNOOPING RETRY-COUNT	88
	48.7 IPV6 MLD SNOOPING GROUP-QUERY-INTERVAL	89
	48.8 IPV6 MLD SNOOPING REPORT-FORWARD	90
	48.9 IPV6 MLD SNOOPING VERSION	91
	48.10 IPV6 MLD SNOOPING FAST-LEAVE	92
	48.11 IPV6 MLD SNOOPING QUERIER	93
	48.12 IPV6 MLD SNOOPING QUERY-INTERVAL	94
	48.13 IPV6 MLD SNOOPING MROUTER	95
	48.14 DEBUG IPV6 MLD SNOOPING	96
	48.15 SHOW IPV6 MLD SNOOPING MROUTER	98
	48.16 SHOW IPV6 MLD SNOOPING GLOBALS	99
	48.17 SHOW IPV6 MLD SNOOPING	101
	48.18 SHOW IPV6 MLD SNOOPING GROUPS	103
	48.19 SHOW IPV6 MLD SNOOPING FORWARDING-DATABASE	105
	48.20 SHOW IPV6 MLD SNOOPING STATISTICS	107
CHAPTER 49:	IGMP	109
	49.1 SET IP IGMP	111
	49.2 IP IGMP IMMEDIATE-LEAVE	112
	49.3 IP IGMP VERSION	113
	49.4 IP IGMP QUERY-INTERVAL	114
	49.5 IP IGMP QUERY-MAX-RESPONSE-TIME	115
	49.6 IP IGMP ROBUSTNESS	116
	49.7 IP IGMP LAST-MEMBER-QUERY-INTERVAL	117
	49.8 IP IGMP STATIC-GROUP	118
	49.9 NO IP IGMP	119
	49.10 DEBUG IP IGMP	120
	49.11 SHOW IP IGMP GLOBAL-CONFIG	121
	49.12 SHOW IP IGMP INTERFACE	122
	49.13 SHOW IP IGMP GROUPS	124
	49.14 SHOW IP IGMP SOURCES	125
	49.15 SHOW IP IGMP STATISTICS	126
CHAPTER 50:	IGMP PROXY	127
	50.1 IP IGMP PROXY-SERVICE	128
	50.2 IP IGMP PROXY SERVICE	129
	50.3 IP IGMP-PROXY MROUTER	130
	50.4 IP IGMP MROUTE PROXY	131
	50.5 IP IGMP-PROXY MROUTER-TIME-OUT	132
	50.6 IP IGMP-PROXY MROUTER-VERSION	133
	50.7 SHOW IP IGMP-PROXY MROUTER	134
	50.8 SHOW IP IGMP-PROXY FORWARDING-DATABASE	135
CHAPTER 51:	PIM	137
	51.1 SET IP PIM	139
	51.2 IP MULTICAST	140

51.3	IP PIM VERSION	141
51.4	SET IP PIM THRESHOLD	142
51.5	SET IP PIM SPT-SWITCHPERIOD	143
51.6	SET IP PIM RP-THRESHOLD	144
51.7	SET IP PIM RP-SWITCHPERIOD	145
51.8	SET IP PIM REGSTOP-RATELIMIT-PERIOD	146
51.9	SET IP PIM PMBR	147
51.10	IP PIM COMPONENT	148
51.11	SET IP PIM STATIC-RP	149
51.12	SET IP PIM STATE-REFRESH ORIGINATION-INTERVAL	150
51.13	IP PIM STATE-REFRESH DISABLE	151
51.14	SET IP PIM SOURCE-ACTIVE INTERVAL	152
51.15	SET MODE	153
51.16	RP-CANDIDATE RP-ADDRESS	154
51.17	RP-CANDIDATE HOLDTIME	155
51.18	RP-STATIC RP-ADDRESS	156
51.19	IP PIM QUERY-INTERVAL	157
51.20	IP PIM MESSAGE-INTERVAL	158
51.21	IP PIM BSR-CANDIDATE - VALUE	159
51.22	IP PIM BSR-CANDIDATE – VLAN	160
51.23	IP PIM COMPONENTID	161
51.24	IP PIM DR-PRIORITY	162
51.25	IP PIM OVERRIDE-INTERVAL	163
51.26	IP PIM LAN-DELAY	164
51.27	SET IP PIM LAN-PRUNE-DELAY	165
51.28	SET IP PIM GRAFT-RETRY INTERVAL	166
51.29	NO IP PIM INTERFACE	167
51.30	DEBUG IP PIM	168
51.31	SHOW IP PIM INTERFACE	169
51.32	SHOW IP PIM NEIGHBOR	171
51.33	SHOW IP PIM RP-CANDIDATE	172
51.34	SHOW IP PIM RP-SET	173
51.35	SHOW IP PIM BSR	174
51.36	SHOW IP PIM RP-STATIC	175
51.37	SHOW IP PIM COMPONENT	176
51.38	SHOW IP PIM THRESHOLDS	177
51.39	SHOW IP PIM MROUTE	178
51.40	SHOW IP PIM REDUNDANCY STATE	180
51.41	SHOW IP PIM REDUNDANCY SHADOW-TABLE	181
CHAPTER 52:	PIMV6	183
52.1	SHOW IP PIM REDUNDANCY STATE	185
52.2	SET IPV6 PIM	186
52.3	SET IP PIM THRESHOLD	187
52.4	SET IP PIM SPT-SWITCHPERIOD	188
52.5	SET IP PIM RP-THRESHOLD	189
52.6	SET IP PIM RP-SWITCHPERIOD	190
52.7	SET IP PIM REGSTOP-RATELIMIT-PERIOD	191
52.8	SET IP PIM PMBR	192
52.9	SET IP PIM STATIC-RP	193
52.10	IP PIM COMPONENT	194
52.11	IPV6 PIM RP-CANDIDATE RP-ADDRESS	195
52.12	IPV6 PIM RP-STATIC RP-ADDRESS	196
52.13	IPV6 PIM QUERY-INTERVAL	197
52.14	IPV6 PIM MESSAGE-INTERVAL	198
52.15	IPV6 PIM BSR-CANDIDATE	199

	52.16 IPV6 PIM COMPONENTID	200
	52.17 IPV6 PIM HELLO-HOLDTIME	201
	52.18 IPV6 PIM DR-PRIORITY	202
	52.19 IPV6 PIM OVERRIDE-INTERVAL	203
	52.20 IPV6 PIM LAN-DELAY	204
	52.21 SET IPV6 PIM LAN-PRUNE-DELAY	205
	52.22 NO IPV6 PIM INTERFACE	206
	52.23 DEBUG IPV6 PIM	207
	52.24 SHOW IPV6 PIM INTERFACE	209
	52.25 SHOW IPV6 PIM NEIGHBOR	211
	52.26 SHOW IPV6 PIM RP-CANDIDATE	212
	52.27 SHOW IPV6 PIM RP-SET	213
	52.28 SHOW IPV6 PIM BSR	214
	52.29 SHOW IPV6 PIM RP-STATIC	215
	52.30 SHOW IPV6 PIM COMPONENT	216
	52.31 SHOW IPV6 PIM THRESHOLDS	217
	52.32 SHOW IPV6 PIM MROUTE	218
	52.33 SHOW IP PIM REDUNDANCY STATE	220
	52.34 SHOW IPV6 PIM REDUNDANCY SHADOW-TABLE	221
CHAPTER 53:	DVMRP	223
	53.1 SET IP DVMRP	224
	53.2 IP DVMRP PRUNE-LIFE-TIME	225
	53.3 DEBUG IP DVMRP	226
	53.4 SHOW IP DVMRP	227
CHAPTER 54:	IPV4 MULTICASTING	229
	54.1 IP MULTICAST ROUTING	230
	54.2 IP MULTICAST-ROUTING	231
	54.3 IP MCAST TTL-THRESHOLD	232
	54.4 IP MCAST RATE-LIMIT	233
	54.5 SHOW IP MROUTE	234
CHAPTER 55:	TAC	235
	55.1 IP MCAST PROFILE	236
	55.2 IP IGMP PROFILE	237
	55.3 SET IP MCAST PROFILING	238
	55.4 PERMIT	239
	55.5 DENY	240
	55.6 RANGE	241
	55.7 PROFILE ACTIVE	242
	55.8 SHOW IP MCAST PROFILE	243
	55.9 DEBUG TACM	244
CHAPTER 56:	RMON	245
	56.1 SET RMON	246
	56.2 RMON COLLECTION HISTORY	247
	56.3 RMON COLLECTION STATS	248
	56.4 RMON EVENT	249
	56.5 RMON ALARM	250
	56.6 SHOW RMON	252
CHAPTER 57:	RMON2	255
	57.1 RMON2	256
	57.2 DEBUG RMON2	257
CHAPTER 58:	DSMON	259
	58.1 DSMON	260
	58.2 DEBUG DSMON	261

CHAPTER 59:	EOAM	263
	59.1 SHUTDOWN ETHERNET-OAM.....	265
	59.2 SET ETHERNET-OAM.....	267
	59.3 ETHERNET-OAM.....	268
	59.4 SET ETHERNET-OAM OUI	269
	59.5 ETHERNET-OAM LINK-MONITOR EVENT-RESEND	270
	59.6 ETHERNET-OAM LINK MONITOR SET	271
	59.7 DEBUG ETHERNET-OAM	272
	59.8 ETHERNET-OAM MODE	274
	59.9 ETHERNET-OAM REMOTE-LOOPBACK – DENY/PERMIT	275
	59.10 ETHERNET-OAM REMOTE-LOOPBACK – ENABLE/DISABLE.....	276
	59.11 ETHERNET-OAM LINK-MONITOR – LINK EVENTS	277
	59.12 ETHERNET-OAM LINK-MONITOR – WINDOW SIZE	278
	59.13 ETHERNET-OAM LINK-MONITOR FRAME WINDOW	280
	59.14 ETHERNET-OAM LINK-MONITOR FRAME-SEC-SUMMARY WINDOW	281
	59.15 ETHERNET-OAM LINK-MONITOR – THRESHOLD ERROR COUNT.....	282
	59.16 ETHERNET-OAM LINK-MONITOR FRAME-SEC-SUMMARY THRESHOLD	284
	59.17 ETHERNET-OAM - CRITICAL-EVENT / DYING-GASP	285
	59.18 CLEAR PORT ETHERNET-OAM - STATISTICS.....	286
	59.19 CLEAR PORT ETHERNET-OAM – EVENT LOG	288
	59.20 SHOW ETHERNET-OAM GLOBAL INFORMATION	290
	59.21 SHOW PORT ETHERNET-OAM.....	291
	59.22 SHOW PORT ETHERNET-OAM - NEIGHBOR	293
	59.23 SHOW PORT ETHERNET-OAM - LOOPBACK-CAPABILITIES	295
	59.24 SHOW PORT ETHERNET-OAM - STATISTICS	297
	59.25 SHOW PORT ETHERNET-OAM - EVENT-LOG	299
CHAPTER 60:	FM	301
	60.1 SET FAULT-MANAGEMENT	303
	60.2 FAULT-MANAGEMENT ETHERNET-OAM REMOTE-LOOPBACK	304
	60.3 FAULT-MANAGEMENT ETHERNET-OAM LINK-MONITOR	306
	60.4 FAULT-MANAGEMENT ETHERNET-OAM	308
	60.5 FAULT-MANAGEMENT ETHERNET-OAM MIB-VARIABLE COUNT	309
	60.6 SET FAULT-MANAGEMENT ETHERNET-OAM MIB-REQUEST	310
	60.7 CLEAR PORT FAULT-MANAGEMENT ETHERNET-OAM.....	311
	60.8 SHUTDOWN FAULT-MANAGEMENT	313
	60.9 DEBUG FAULT-MANAGEMENT	314
	60.10 SHOW FAULT-MANAGEMENT GLOBAL INFORMATION	316
	60.11 SHOW PORT FAULT-MANAGEMENT EOAM – MIB VARIABLE RESPONSE	317
	60.12 SHOW PORT FAULT-MANAGEMENT ETHERNET-OAM	319
	60.13 SHOW PORT FAULT-MANAGEMENT ETHERNET-OAM – REMOTE LOOPBACK....	321
CHAPTER 61:	RM	323
	61.1 REDUNDANCY.....	324
	61.2 HB-INTERVAL.....	325
	61.3 PEER-DEAD-INTERVAL	326
	61.4 PEER-DEAD-INTERVAL-MULTIPLIER.....	327
	61.5 REDUNDANCY FORCE-SWITCHOVER	328
	61.6 DEBUG RMGR	329
	61.7 SHOW REDUNDANCY	330
CHAPTER 62:	PTP	331
	62.1 SHUTDOWN PTP.....	333
	62.2 PTP - VRF SWITCH	334
	62.3 PTP ENABLE DISABLE	335
	62.4 PTP PRIMARY-CONTEXT	336
	62.5 PTP NOTIFICATION.....	337

62.6	PTP PRIMARY-DOMAIN	339
62.7	PTP TWO-STEP-CLOCK.....	340
62.8	PTP CLOCK PORTS	341
62.9	PTP PORT	342
62.10	PTP MODE	343
62.11	PTP SLAVE	345
62.12	PTP PATHTRACE	346
62.13	PTP ALTERNATE-TIME-SCALE KEY	347
62.14	PTP ALTERNATE-TIME-SCALE ENABLE KEY.....	348
62.15	PTP ALTERNATE-TIME-SCALE KEY	349
62.16	PTP ACCEPTABLE-MASTER PROTOCOL.....	350
62.17	PTP ALTERNATE-MASTER	351
62.18	PTP ACCEPTABLE-MASTER ENABLE	352
62.19	PTP MAX ALTERNATE-MASTERS	353
62.20	PTP	354
62.21	PTP - IPV6.....	357
62.22	PTP ALTERNATE-MASTER - IPV6	360
62.23	PTP ACCEPTABLE-MASTER ENABLE - IPV6	361
62.24	PTP MAX ALTERNATE-MASTERS - IPV6	362
62.25	SHOW PTP GLOBAL INFO	363
62.26	SHOW PTP VRF SWITCH INFO	364
62.27	SHOW PTP CLOCK	365
62.28	SHOW PTP FOREIGN-MASTER-RECORD	366
62.29	SHOW PTP PARENT	367
62.30	SHOW PTP PORT	368
62.31	SHOW PTP COUNTERS	370
62.32	SHOW PTP TIME-PROPERTY.....	371
62.33	SHOW PTP CURRENT	372
62.34	SHOW PTP ACCEPTABLE MASTERS	373
62.35	SHOW PTP ALTERNATE TIME-SCALE.....	374
62.36	DEBUG PTP	375
CHAPTER 63:	LAYER 4 SWITCHING	377
63.1	LAYER4 SWITCH.....	378
63.2	SHOW LAYER4 SWITCH	379

Chapter

47

IGMP Snooping

Internet Group Multicast Protocol, (IGMP) is the protocol, a host uses to inform a router when it joins (or leaves) an Internet multicast group. IGMP is only used on a local network; a router must use another multicast routing protocol to inform other routers of group membership. IGMP Snooping (IGS) is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers. In IGS, a host computer uses IGMP to inform a router that it intends to listen to a specific multicast address. If another computer snoops such packets, it can learn the multicast sessions to which other computers on the local network are listening. The multicast packet transfer happens only between the source and the destination computers. Broadcasting of packets is avoided. IGMP snooping significantly reduces traffic from streaming media and other bandwidth-intensive IP multicast applications.



The list of CLI commands for the configuration of IGS are common to both **Single Instance** and **Multiple Instance** except for a difference in the prompt that appears for the Switch with Multiple Instance support.

The prompt for the **Global Configuration Mode** is,

```
iss(config)#
```

The list of CLI commands for the configuration of IGS is as follows:

- ip igmp snooping
- ip igmp snooping proxy-reporting
- snooping multicast-forwarding-mode
- ip igmp snooping mrouter-time-out / ip igmp querier-timeout
- ip igmp snooping port-purge-interval / ip igmp snooping source-only learning age-timer
- ip igmp snooping report-suppression interval
- ip igmp snooping retry-count

- ip igmp snooping group-query-interval
- ip igmp snooping report-forward
- ip igmp snooping query-forward
- ip igmp snooping version
- ip igmp snooping fast-leave / ip igmp snooping vlan - immediate leave
- ip igmp snooping querier
- ip igmp snooping query-interval
- ip igmp snooping startup-query-interval
- ip igmp snooping startup-query-count
- ip igmp snooping other-querier-present-interval
- ip igmp snooping vlan mrouter
- shutdown snooping
- debug ip igmp snooping
- snooping leave-process config-level
- ip igmp snooping enhanced-mode
- ip igmp snooping sparse-mode
- snooping report-process config-level
- ip igmp snooping multicast-vlan / mvr
- ip igmp snooping filter
- ip igmp snooping blocked-router
- ip igmp snooping multicast-vlan profile
- ip igmp snooping leavemode
- ip igmp snooping ratelimit
- ip igmp snooping limit
- ip igmp snooping filter-profileid
- ip igmp snooping proxy
- ip igmp snooping max-response-code
- ip igmp snooping mrouter-port -time-out
- ip igmp snooping mrouter-port-version
- show ip igmp snooping mrouter
- show ip igmp snooping mrouter - Redundancy
- show ip igmp snooping globals
- show ip igmp snooping
- show ip igmp snooping - Redundancy
- show ip igmp snooping groups

- show ip igmp snooping forwarding-database
- show ip igmp snooping forwarding-database - Redundancy
- show ip igmp snooping statistics
- show ip igmp snooping blocked-router
- show ip igmp snooping multicast-receivers
- show ip igmp snooping port-cfg
- show ip igmp snooping multicast-vlan

47.1 ip igmp snooping

This command enables IGMP snooping in the switch/ a specific VLAN. When snooping is enabled in a switch or interface, it learns the hosts intention to listen to a specific multicast address. When the switch receives any packet from the specified multicast address, it forwards the packet to the host listening for that address. Broadcasting is avoided to save bandwidth. When IGMP snooping is enabled globally, it is enabled in all the existing VLAN interfaces.

The no form of the command disables IGMP snooping in the switch/a specific VLAN.

When IGMP snooping is disabled globally, it is disabled in all the existing VLAN interfaces.

Global Configuration Mode

```
ip igmp snooping [vlan<vlanid(1-4094)>]
no ip igmp snooping [vlan<vlanid(1-4094)>]
```

Config-VLAN Mode

```
ip igmp snooping
no ip igmp snooping
```

Syntax description	vlan<vlanid>	Configures the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
---------------------------	---------------------------	--

Mode	Global Configuration Mode / Config-VLAN Mode
-------------	--

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	IGMP snooping is globally disabled, and in all VLANs.
-----------------	---

Example	<pre>iss(config)# ip igmp snooping iss(config-vlan)# ip igmp snooping</pre>
----------------	---



GMRP has to be disabled for the IGMP snooping to be enabled.

**Related
Commands**

- **shutdown snooping** - Shuts down IGMP snooping in the switch.
- **show ip igmp snooping** - Displays IGMP snooping information for all VLANs or a specific VLAN.
- **show ip igmp snooping globals** - Displays the IGMP snooping information for all VLANs or a specific VLAN.
- **snooping multicast-forwarding-mode** – Specifies the snooping multicast forwarding mode.
- **show ip igmp snooping multicast-receivers** – Displays IGMP multicast host information for all VLANs or a specific VLAN or specific VLAN and group address for a given switch or for all switches (if no switch is specified).

-

47.2 ip igmp snooping proxy-reporting

This command enables proxy reporting in the IGMP snooping switch. When enabled, the switch supports the multicast router to learn the membership information of the multicast group. It forwards the multicast packets based on group membership information. The proxy-reporting switch acts as a querier to the downstream hosts. It sends proxy-reporting to upstream queriers. The no form of the command disables proxy reporting in the IGMP snooping switch.

ip igmp snooping proxy-reporting

no ip igmp snooping proxy-reporting

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Proxy-reporting is enabled

Example `iss(config)# ip igmp snooping proxy-reporting`



Proxy reporting can be enabled in the IGMP snooping switch only if the proxy is disabled in the switch.

- Related Command**
- **show ip igmp snooping globals** - Displays the IGMP snooping information for all VLANs or a specific VLAN
 - **no ip igmp snooping proxy** – Disables proxy in the IGMP snooping switch.

47.3 snooping multicast-forwarding-mode

This command specifies the snooping multicast forwarding mode (IP based or MAC based). When ip mode is selected, and PIM and IGS are enabled, the L3 bitmap in the IPMC table is updated by PIM. The corresponding L2 bitmap is updated by querying the IGS to obtain Portlist. When PIM is disabled, IGS updates the L2 bitmap in the IPMC table directly. When the mode is MAC based, the L2 bitmap is updated by PIM which queries the VLAN to obtain Portlist. When PIM is disabled, the IGS updates the L2 bitmap directly.

snooping multicast-forwarding-mode {ip | mac}

Syntax Description	ip	- Configures the multicast forwarding mode as IP Address based. The PIM queries the IGS module to obtain the Portlist.
	mac	- Configures the multicast forwarding mode as MAC Address based. The PIM queries the VLAN to obtain the Portlist.
Mode	Global Configuration Mode	
Package	Workgroup, Enterprise and Metro	
Defaults	ip	
Example	iss(config)# snooping multicast-forwarding-mode mac	
Related Command	• show ip igmp snooping globals - Displays the IGMP snooping information for all VLANs or a specific VLAN	
	• ip igmp snooping enhanced-mode - Enables/disables snooping system enhanced mode in the switch.	

47.4 ip igmp snooping mrouter-time-out

This command sets the IGMP snooping router port purge time-out . Snooping learns the available router ports. For each router port learnt the timer is initiated. The routers send control messages to the ports. If the router ports receive such control messages, the timer is restarted. If no message is received by the router ports before the timer expires, the router port entry is purged.

The no form of the command sets the IGMP snooping router port purge time-out to default value.

```
ip igmp snooping mrouter-time-out <(60 - 600) seconds>
```

```
no ip igmp snooping mrouter-time-out
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 125

Example iss(config)#ip igmp snooping mrouter-time-out 70

Related Command

- **show ip igmp snooping mrouter** - Displays the router ports for all VLANs or specific VLAN
- **show ip igmp snooping globals** - Displays the global information of IGMP snooping

47.5 ip igmp querier-timeout

This command sets the IGMP snooping router port purge time-out after which the port gets deleted, if no IGMP router control packets are received. The purge time-out value ranges between 60 and 600 seconds.

This command is a standardized implementation of the existing command; **ip igmp snooping mrouter-time-out**. It operates similar to the existing command.

ip igmp querier-timeout <(60 - 600) seconds>

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 125

Example `iss(config)#ip igmp querier-timeout 70`

Related Command

- **show ip igmp snooping mrouter** - Displays the router ports for all VLANs or specific VLAN
- **show ip igmp snooping globals** - Displays the global information of IGMP snooping

47.6 ip igmp snooping port-purge-interval

This command configures the IGMP snooping port purge time interval for the interface. When the port receives reports from hosts, the timer is initiated and continues till the set period of time. If the port receives another report before the timer expires, the timer is restarted. If the port does not receive any report from hosts till the timer expires, the port entry is purged from the multicast database. The no form of the command sets the IGMP snooping port purge time to default value.

```
ip igmp snooping port-purge-interval <(130 - 1225) seconds>
```

```
no ip igmp snooping port-purge-interval
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 260

Example iss (config)# ip igmp snooping port-purge-interval 150

Related Command **show ip igmp snooping globals** - Displays the IGMP snooping information for all VLANs or a specific VLAN

47.7 ip igmp snooping source-only learning age-timer

This command sets the IGMP snooping port purge time interval after which the port gets deleted, if no IGMP reports are received. The purge time interval value ranges between 130 and 1225 seconds. The no form of the command sets the IGMP snooping port purge time to the default value.

This command is a standardized implementation of the existing command; **ip igmp snooping port-purge-interval**. It operates similar to the existing command.

```
ip igmp snooping source-only learning age-timer <short (130-1225)>
```

```
no ip igmp snooping source-only learning age-timer
```

Mode	Global Configuration Mode
-------------	---------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	260
-----------------	-----

Example	iss (config)# ip igmp snooping source-only learning age-timer 200
----------------	---

Related Command	show ip igmp snooping globals - Displays the IGMP snooping information for all VLANs or a specific VLAN
------------------------	--

47.8 ip igmp snooping report-suppression interval

This command sets the IGMP snooping report-suppression time interval. The switch forwards a IGMPv2 report message to the multicast group. A timer is started immediately after forwarding the report message and runs for set period of time. During this interval the switch does not forward another IGMPv2 report message addressed to the same multicast group to the router ports.

The no form of the command sets the IGMP snooping report-suppression interval time to the default value.

```
ip igmp snooping report-suppression-interval <(1 - 25) seconds>
```

```
no ip igmp snooping report-suppression-interval
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 5

Example iss(config)# ip igmp snooping report-suppression-interval 20



The ip igmp snooping report-suppression-interval is used only when the proxy and proxy-reporting are disabled.

Related Command **show ip igmp snooping globals** - Displays the IGMP snooping information for all VLANs or a specific VLAN

47.9 ip igmp snooping retry-count

This command sets the maximum number of group specific queries sent by the switch to check if there are any interested v2 receivers for the group when it receives a leave message in the proxy/ proxy-reporting mode. The port is deleted from the group membership information in the forwarding database if the maximum retry count exceeds set number.

The no form of the command sets the number of group specific queries sent by the switch on reception of leave message to default value.

```
ip igmp snooping retry-count <1 - 5>
```

```
no ip igmp snooping retry-count
```

Mode	Global Configuration Mode
-------------	---------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	2
-----------------	---

Example	iss (config)# ip igmp snooping retry-count 4
----------------	--

Related Command	show ip igmp snooping globals - Displays the IGMP snooping information for all VLANs or a specific VLAN
------------------------	--

47.10 ip igmp snooping group-query-interval

This command sets the time interval after which the switch sends a group specific query to find out if there are any interested receivers in the group when it receives a leave message. If it does not receive a response from the group, the port is removed from the group membership information in the forwarding database.

The no form of the commands sets the group specific query interval time to default value.

```
ip igmp snooping group-query-interval <2-5> seconds>
```

```
no ip igmp snooping group-query-interval
```

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 2

Example iss(config)# ip igmp snooping group-query-interval 3

Related Commands

- **show ip igmp snooping globals** - Displays the IGMP snooping information for all VLANs or a specific VLAN
- **show ip igmp snooping statistics** - Displays IGMP snooping statistics for all VLANs or a specific VLAN
- **show ip igmp snooping groups** - Displays IGMP group information for all VLANs or a specific VLAN

47.11 ip igmp snooping report-forward

This command configures the IGMP reports to be forwarded to all ports, router ports of a VLAN or non-edge ports. The configuration enables the switch to forward IGMP report messages to the selected ports thus avoiding flooding of the network. This configuration is not valid in proxy or proxy reporting mode.

The no form of the command sets IGMP report-forwarding status to default value.

```
ip igmp snooping report-forward {all-ports | router-ports | non-edge-ports }
no ip igmp snooping report-forward
```

Syntax Description	all-ports	-	Configures the IGMP reports to be forwarded to all the ports of a VLAN
---------------------------	------------------	---	--

	router-ports	-	Configures the IGMP reports to be forwarded only to router ports of a VLAN
--	---------------------	---	--

	non-edge-ports	-	Configures the IGMP reports to be forwarded only to STP non edge ports
--	-----------------------	---	--

Mode	Global Configuration Mode
-------------	---------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	router-ports
-----------------	--------------

Example	iss(config)# ip igmp snooping report-forward all-ports
----------------	--



- This configuration is not valid in proxy or proxy-reporting mode.
- In snooping mode, snooping module will forward reports only on router ports by default.

Related Command	show ip igmp snooping globals - Displays the IGMP snooping information for all VLANs or a specific VLAN
------------------------	--

47.12 ip igmp snooping query-forward

This command configures the IGMP queries to be forwarded to all Vlan member ports or only to non-router ports. This configuration directs the queries to the selected ports to avoid flooding of the network. The queries are forwarded to multicast groups. If the Vlan module is enabled, IGMP snooping sends and receives the multicast packets through Vlan module. When Vlan is disabled, it sends the multicast packets through Bridge initialization/shutdown submodule.

```
ip igmp snooping query-forward {all-ports | non-router-ports}
```

Syntax Description	all-ports	- Configures the IGMP query forward administrative control status as all VLAN member ports. This is done to find out if there are any interested listeners in the network.
	non-router-ports	- Configures the IGMP query forward administrative control status as non-router ports only. This is done to reduce the traffic in the network.
Mode	Global Configuration Mode	
Package	Workgroup, Enterprise and Metro	
Defaults	non-router-ports	
Example	iss(config)# ip igmp snooping query-forward all-ports	
Related Command	<ul style="list-style-type: none"> • show ip igmp snooping globals - Displays the IGMP snooping information for all VLANs or a specific VLAN. 	

47.13 ip igmp snooping version

This command configures the operating version of the IGMP snooping switch for a specific VLAN. The version can be set manually to execute condition specific commands..

```
ip igmp snooping version { v1 |v2 | v3}
```

Syntax Description	v1	-	Configures the version as IGMP snooping Version 1.
---------------------------	----	---	--

	v2	-	Configures the version IGMP snooping Version 2.
--	----	---	---

	v3	-	Configures the version IGMP snooping Version 3.
--	----	---	---

Mode	Config-VLAN Mode
-------------	------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	v3
-----------------	----

Example	iss(config-vlan)#ip igmp snooping version v2
----------------	--

Related Command	show ip igmp snooping - Displays IGMP snooping information for all VLANs or a specific VLAN
------------------------	--

47.14 ip igmp snooping fast-leave

This command enables fast leave processing for a specific VLAN. When the fast leave feature is enabled, a port information is removed from a multicast group entry immediately after fast leave message is received. The no form of the command disables fast leave processing for a specific VLAN.

ip igmp snooping fast-leave

no ip igmp snooping fast-leave

Mode Config-VLAN Mode

Package Workgroup, Enterprise and Metro

Defaults Disabled

Example iss (config-vlan)# ip igmp snooping fast-leave



Fast leave processing will be enabled in the VLAN, only if the IGMP snooping is globally enabled.

Related Command

- **show ip igmp snooping** - Displays IGMP snooping information for all VLANs or a specific VLAN
- **show ip igmp snooping globals** - Displays the global information of IGMP snooping

47.15 ip igmp snooping vlan - immediate leave

This command enables fast leave processing for a specific VLAN. The no form of the command disables fast leave processing for a specific VLAN. ID of the VLAN ranges between 1 and 4094.

This command is a standardized implementation of the existing command; **ip igmp snooping fast-leave** and also enables IGMP snooping in that particular VLAN if IGMP snooping is globally enabled.. It operates similar to the existing command.

The fast leave processing and the IGMP snooping will not be enabled in the VLAN even if the IGMP snooping is globally enabled, once the IGMP snooping is disabled in the VLAN by the user. User must again enable IGMP snooping in the VLAN for enabling the fast leave process.

```
ip igmp snooping vlan <vlanid(1-4094)> immediate-leave
```

```
no ip igmp snooping vlan <vlanid(1-4094)> immediate-leave
```

Mode	Global Configuration Mode
------	---------------------------

Package	Workgroup, Enterprise and Metro
---------	---------------------------------

Defaults	By default, fast leave processing is disabled in all the VLANs
----------	--

Example	iss (config)# ip igmp snooping vlan 1 immediate-leave
---------	---



Fast leave processing will be enabled in the VLAN, only if the IGMP snooping is globally enabled.

Related Command

- **show ip igmp snooping** - Displays IGMP snooping information for all VLANs or a specific VLAN.
- **show ip igmp snooping globals** - Displays the global information of IGMP snooping.

47.16 ip igmp snooping querier

This commands configures the IGMP snooping switch as a querier for a specific VLAN. When configured as a querier, the switch sends IGMP query messages. The query messages will be suppressed if there are any routers in the network. The no form of the command configures the IGMP snooping switch as non-querier for a specific VLAN.

ip igmp snooping querier

no ip igmp snooping querier

Mode Config-VLAN Mode

Package Workgroup, Enterprise and Metro

Defaults Non-querier

Example iss (config-vlan)# ip igmp snooping querier

Related Command **show ip igmp snooping** - Displays IGMP snooping information for all VLANs or a specific VLAN

47.17 ip igmp snooping query-interval

This command sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN. The switch sends querier messages in proxy mode and proxy-reporting mode to all downstream interfaces for this time interval. The value range is between 60 to 600 seconds.

The no form of the command sets the IGMP querier interval to default value.

```
ip igmp snooping query-interval <(60 - 600) seconds>
```

```
no ip igmp snooping query-interval
```

Mode	Config-VLAN Mode
-------------	------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	125
-----------------	-----

Example	iss (config-vlan) # ip igmp snooping query-interval 200
----------------	---



The switch must be configured as a querier for this configuration to be imposed.

In proxy reporting mode, general queries are sent on all downstream interfaces with this interval only if the switch is the Querier.

In proxy mode, general queries will be sent on all downstream interfaces with this interval.

Related Command	show ip igmp snooping - Displays IGMP snooping information for all VLANs or a specific VLAN
------------------------	--

47.18 ip igmp snooping startup-query-interval

This command sets the time interval between the general query messages sent by the IGMP snooping switch, during startup of the querier election process. This time interval ranges between 15 and 150 seconds and should be less than or equal to query interval/ 4.

The no form of the command sets the IGMP startup query interval to the default value.

```
ip igmp snooping startup-query-interval <(15 - 150) seconds>
```

```
no ip igmp snooping startup-query-interval
```

Mode Config-VLAN Mode

Package Workgroup, Enterprise and Metro

Defaults 32

Example iss(config-vlan) # ip igmp snooping startup-query-interval 100



The switch should be configured as querier for the startup query interval command to produce results.

The startup query interval should be less than or equal to ¼ of the query interval.

Related Command

- **ip igmp snooping query-interval** - Sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN
- **show ip igmp snooping querier** - Displays IGMP snooping information for all VLANs or a specific VLAN
- **show ip igmp snooping** - Displays IGMP snooping information for all VLANs or a specific VLAN for a given context or for all the contexts.

47.19 ip igmp snooping startup-query-count

This command sets the maximum number of general query messages sent out on switch startup, when the switch is configured as a querier. This value ranges between two and five. Startup query messages are sent to announce the presence of the switch along with its identity. The startup query count is manually configured to change the existing count.

The no form of the command sets the number of general query messages sent out on switch startup, when the switch is configured as a querier to default value.

```
ip igmp snooping startup-query-count <2 - 5>
```

```
no ip igmp snooping startup-query-count
```

Mode Config-VLAN Mode

Package Workgroup, Enterprise and Metro

Defaults 2

Example iss (config-vlan) # ip igmp snooping startup-query-count 4



The switch should be configured as a querier for startup query count command to provide result.

Related Command

- **show ip igmp snooping** - Displays IGMP snooping information for all VLANs or a specific VLAN
- **ip igmp snooping querier** - Configures the IGMP snooping switch as a querier for a specific VLAN
- **ip igmp snooping query-interval** - Command sets the time period with which the general queries are sent by the IGMP snooping switch

47.20 ip igmp snooping other-querier-present-interval

This command sets the maximum time interval to decide that another querier is present in the network. This time interval ranges between 120 and 1215 seconds. Within this time interval if the querier receives response from another querier, then the one with a higher IP address is announced as the querier for the network. The other querier present interval must be greater than or equal to ((Robustness Variable * Query Interval) + (Query Response Interval/2)). Here, Robustness value is 2.

The no form of the command resets this interval to default value..

```
ip igmp snooping other-querier-present-interval <value (120-1215) seconds>
```

```
no ip igmp snooping other-querier-present-interval
```

Mode Config-VLAN Mode

Package Workgroup, Enterprise and Metro

Defaults 255

Example

```
iss(config-vlan) # ip igmp snooping other-querier-present-interval 200
```



The switch should be configured as a querier for the other querier present command to be effective.

The other querier present interval must be greater than or equal to ((Robustness Variable * Query Interval) + (Query Response Interval/2)).

Related Command

- **ip igmp snooping query-interval** - Sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN.
- **ip igmp snooping max-response-code** - Sets the maximum response code inserted in general queries send to host.
- **show ip igmp snooping** - Displays IGMP snooping information for all VLANs or a specific VLAN.

47.21 ip igmp snooping mrouter

This command configures a list of ports as routerports in a VLAN. Any IGMP message received on a switch is forwarded only on router-ports and not on host ports. The IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network. The no form of the command deletes the statically configured router ports for a VLAN.

```
ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...>
```

```
no ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...>
```

Mode Config-VLAN Mode

Package Workgroup, Enterprise and Metro

Example

```
iss (config-vlan)# ip igmp snooping mrouter gigabitethernet 0/1-3
```

Related Command

- **show ip igmp snooping mrouter** - Displays the router ports for all VLANs or specific VLAN.
- **ip igmp snooping mrouter-port -time-out** - Configures the router port purge time-out interval for a VLAN.
- **ip igmp snooping mrouter-port-version** - Configures the operating version of the router port for a VLAN.

47.22 ip igmp snooping vlan mrouter

This command configures statically the router ports for a VLAN and the no form of the command deletes the statically configured router ports for a VLAN.

This command is a standardized implementation of the existing command; **ip igmp snooping mrouter**. It operates similar to the existing command.

```
ip igmp snooping vlan <vlanid (1-4094)> mrouter <ifXtype> <0/a-b, 0/c, ...>
```

```
no ip igmp snooping vlan <vlanid (1-4094)> mrouter <ifXtype> <0/a-b, 0/c, ...>
```

Syntax Description	vlanid	- ID of the VLAN for which the router ports should be configured statically. This value ranges between 1 and 4094.
	ifXtype	- Type of the interface. The values can be: <ul style="list-style-type: none"> • gigabitethernet • fastethernet
	<0/a-b, 0/c, ...>	- Interface list which specifies the particular slot and the concerned port number.
Mode	Global Configuration Mode	
Package	Workgroup, Enterprise and Metro	
Example	iss(config)# ip igmp snooping vlan 1 mrouter gigabitethernet 0/1	
Related Command	<ul style="list-style-type: none"> • show ip igmp snooping mrouter - Displays the router ports for all VLANs or specific VLAN • ip igmp snooping mrouter-port -time-out - Configures the router port purge time-out interval for a VLAN • ip igmp snooping mrouter-port-version - Configures the operating version of the router port for a VLAN 	

47.23 shutdown snooping

This command shuts down snooping in the switch. When the user does not require the IGMP snooping module to be running, it can be shut down. When shutdown, all resources acquired by the Snooping Module are released to the system. For the IGS feature to be functional on the switch, the 'system-control' status must be set as 'start' and the 'state' must be 'enabled'. The no form of the command starts and enables snooping in the switch.

shutdown snooping

no shutdown snooping

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	no shutdown snooping
Example	<code>iss(config)# shutdown snooping</code>



- Snooping cannot be started in the switch, if the base bridge mode is configured as transparent bridging.

Related Command

- **base bridge-mode** - Configures the mode in which the VLAN feature should operate on the switch.
- **ip igmp snooping** - Enables IGMP snooping in the switch/a specific VLAN

47.24 debug ip igmp snooping

This command configures the various debug and trace statements to handle error and event management available in the igmp snooping module. The traces are enabled by passing the necessary parameters.

The no form of the command resets debug options for IGMP snooping module.

```
debug ip igmp snooping {[init][resources][tmr][src][grp][qry]
[vlan][pkt][fwd][mgmt][redundancy] | all } [switch <switch_name>]
```

```
no debug ip igmp snooping {[init][resources][tmr][src][grp][qry]
[vlan][pkt][fwd][mgmt][redundancy] | all } [switch <switch_name>]
```

Syntax Description	init	- Generates Init and Shutdown trace messages at the instances when the module is initiated or shutdown. The information is logged in a file.
	resources	- Generates System Resources management trace messages when there is a change in the resource status. The information is logged in a file.
	tmr	- Generates Timer trace messages at the instances where timers are involved. The information is logged in a file.
	src	- Generates trace messages when Source Information is involved.
	grp	- Generates trace messages when Group Information is involved.
	qry	- Generates trace messages when Query messages are sent or received.
	vlan	- Generates trace messages when VLAN related Information is involved.
	pkt	- Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.
	fwd	- Generates traces messages when forwarding Database is involved.
	mgmt	- Generates debug statements for management plane functionality traces.

	redundancy	- Generates debug statements for redundancy code flow traces. This trace is generated when there is a failure in redundancy processing.
	all	- Generates all types of trace messages
	switch <switch_name>	- Generates switch related trace messages.
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	
Defaults	Debugging is Disabled.	
Example	iss# debug ip igmp snooping fwd	
Related Command	show debugging - Displays state of each debugging option	

47.25 snooping leave-process config-level

This command specifies the level of configuring the leave processing mechanisms. When the switch intercepts a leave group message on a switch port, it normally sends a query to that multicast group through the same switch port. If no hosts respond to the query and no multicast routers have been discovered on the switch port, that port is removed from the multicast group.

snooping leave-process config-level {vlan | port}

Syntax Description	vlan	-	Configures the leave mechanism at the Vlan level. In Vlan based leave processing mode, the fast leave functionality configurable per vlan or normal leave configurations are available for processing leave messages.
	port	-	Configures the leave mechanism at port level. In Port based leave processing mode, the explicit host tracking functionality, the fast leave functionality or normal leave configurable on a interface are used for processing the leave messages.
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	vlan		
Example	<code>iss(config)# snooping leave-process config-level port</code>		
Related Command	<ul style="list-style-type: none"> • ip igmp snooping leavemode – Configures the port leave mode for an interface. 		
	<ul style="list-style-type: none"> • show ip igmp snooping globals – Displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switch (if switch is not specified) 		

47.26 ip igmp snooping enhanced-mode

This command configures snooping system enhanced mode in the switch. It is a mode of operation provided to enhance the operation of IGMP snooping module to duplicate Multicast traffic by learning Multicast group entries based on the Port and Inner Vlan. This mode of operation is applied when the down stream devices are less intelligent or not capable of duplicating Multicast traffic.

```
ip igmp snooping enhanced-mode { enable | disable }
```

Syntax Description	enable	- Enables snooping system enhanced mode in the switch.
	disable	- Disables snooping system enhanced mode in the switch.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults disable

Example iss(config)# ip igmp snooping enhanced-mode enable




- Enhanced mode is in enabled state only when the snooping mode is set as IP Based.

Related Command	<ul style="list-style-type: none"> snooping multicast-forwarding-mode – Specifies the snooping multicast forwarding mode. show ip igmp snooping globals – Displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switch (if switch is not specified). ip igmp snooping leavemode – Configures the port leave mode for an interface. ip igmp snooping ratelimit – Configures the rate limit for a downstream interface in units of the number of IGMP packets per second. ip igmp snooping limit – Configures the maximum limit type for an interface. ip igmp snooping filter-profileId – Configures the multicast profile index for a downstream interface.
------------------------	---

47.27 ip igmp snooping sparse-mode

This command configures snooping system sparse mode in the switch. In the sparse mode, the IGS module drops the unknown multicast traffic when there is no listener for the multicast data. In the non-sparse-mode, the IGS module forwards the unknown multicast traffic. The multicast data gets flooded to the member port of vlan.

```
ip igmp snooping sparse-mode { enable | disable }
```

Syntax Description	enable	-	Enables snooping system sparse mode in the switch. Drops unknown multicast packets.
	disable	-	Disables snooping system sparse mode in the switch. Floods unknown multicast packets.
Mode	Global Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	disable		
Example	iss(config)# ip igmp snooping sparse-mode enable		
	Sparse mode is in enabled state only when the snooping mode is set as MAC Based		
Related Command	<ul style="list-style-type: none"> • show ip igmp snooping globals – Displays the IGMP snooping information for all VLANs or a specific VLAN. 		

47.28 snooping report-process config-level

This command sets the configuration-level for report processing as non-router ports or as all ports.

```
snooping report-process config-level {non-router-ports | all-ports}
```

Syntax Description	non-router-ports	- The incoming report messages are processed only in the non-router ports. Report message received on the router ports are not processed in this configuration.
	all-ports	- The incoming report messages are processed in all the ports inclusive of router ports.
Mode	Global Configuration Mode	
Package	Workgroup, Enterprise and Metro	
Defaults	non-router-ports	
Example	<pre>iss(config)# snooping report-process config-level all-ports</pre>	
Related Command	<ul style="list-style-type: none">• show ip igmp snooping globals - Displays the IGMP snooping information for all VLANs or a specific VLAN.	

47.29 ip igmp snooping multicast-vlan

This command configures the multicast VLAN feature on a port. Multicast VLAN feature is used for applications where wide-scale deployment of multicast traffic is necessary. MVLAN registration allows a subscriber on a port to subscribe and unsubscribe to a particular multicast stream on any of the multicast VLANs. Multicast VLANs enable efficient multicast data flow in separate M-VLANs, while normal data flows through VLANs.

ip igmp snooping multicast-vlan {enable|disable}

Syntax Description	enable	- Enables the multicast Vlan feature. Router sends a single copy of the data for the particular MVLAN, instead of forwarding a separate copy of the multicast data to each VLAN. This saves the network bandwidth
	disable	- Disables the multicast Vlan feature. A separate copy of the multicast data has to be forwarded from the router in the absence of M-VLAN.
Mode	Global Configuration Mode	
Package	Workgroup, Enterprise and Metro	
Defaults	disable	
Example	iss(config)# ip igmp snooping multicast-vlan enable	
Related Command	<ul style="list-style-type: none"> • show ip igmp snooping multicast-vlan – Displays multicast VLAN statistics in a switch and displays various profiles mapped to the multicast VLANs. • show ip igmp snooping globals – Displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switch (if switch is not specified) 	

47.30 mvr

This command enables the multicast VLAN feature. The no form of this command disables the multicast VLAN feature.

This command is a standardized implementation of the existing command; **ip igmp snooping multicast-vlan**. It operates similar to the existing command.

mvr

no mvr

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults By default, multicast VLAN feature is disabled.

Example `iss(config)# mvr`

Related Command

- **show ip igmp snooping multicast-vlan** – Displays multicast VLAN statistics in a switch and displays various profiles mapped to the multicast VLANs
- **show ip igmp snooping globals** – Displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switch (if switch is not specified)

47.31 ip igmp snooping filter

This command configures the IGMP snooping filter. The IGS filtering feature restricts channel registration from being added to the database. In transparent snooping, the filtered packet will not be added to the snooping database but will be forwarded upstream. When disabled, all the filter related configurations remain but the incoming reports will not be subject to filtering. IGS module programs the hardware to remove the configured rate limit. It flushes all the registrations learnt through a port if a threshold limit is configured for this interface.

The no form of the command disables the IGMP snooping filter.

ip igmp snooping filter

no ip igmp snooping filter

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults disabled.

Example `iss(config)# ip igmp snooping filter`

Related Command

- **show ip igmp snooping globals** – Displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switch (if switch is not specified).
- **ip igmp snooping ratelimit** – Configures the rate limit for a downstream interface in units of the number of IGMP packets per second.
- **ip igmp snooping limit** – Configures the maximum limit type for an interface.
- **ip igmp snooping filter-profileId** – Configures the multicast profile index for a downstream interface.

47.32 ip igmp snooping blocked-router

This command configures a static router-port as blocked router port. When configured as a blocked router, the queries, PIM DVMRP and data messages are discarded, The corresponding port entry is removed from the forwarding database. The ports to be configured as blocked router ports, must not be configured as static router ports.

The no form of the command resets the blocked router ports to normal router port.

```
ip igmp snooping blocked-router <interface-type> <0/a-b, 0/c, ...>
```

```
no ip igmp snooping blocked-router <interface-type> <0/a-b, 0/c, ...>
```

Syntax Description	<interface-type> - Configures the type of interface to be employed on the port.
	<0/a-b, 0/c, ...> - Configures the list of router-ports to be set as blocked. The interface ids are given as an array

Mode Config-VLAN Mode

Package Workgroup, Enterprise and Metro

Example iss (config-vlan)# ip igmp snooping blocked-router
gigabitethernet 0/4-5



The ports to be configured as blocked router ports, must not be configured as static router ports.

Related Command **show ip igmp snooping blocked-router** – Displays the blocked router ports for all VLANs or a specific VLAN for a given switch or for all the switches (if no switch is specified)

47.33 ip igmp snooping multicast-vlan profile

This command configures profile ID to VLAN mapping for multicast VLAN classification. The switch is configured with list of entries such as multicast group, multicast source and filtermode. These entries are maintained in access profiles. Each profile is associated with a particular vlan whis is categorized as multicast vlan. When any untagged report or leave message is received (that is, packet with no tag in a customer bridge or packet with no S-tag in a provider or 802.1ad bridge), and if the group and source address in the received packet matches any rule in this profile, then the received packet is classified to be associated to the VLAN (that is, multicast VLAN) to which the profile is mapped.

The no form of the command removes the profile ID to VLAN mapping for multicast VLAN classification.

```
ip igmp snooping multicast-vlan profile <Profile ID (0-4294967295)>
```

```
no ip igmp snooping multicast-vlan profile
```

Syntax Description	<Profile ID>	- Configures the multicast profile ID for a particular VLAN. This value ranges between 0 and 4294967295.
---------------------------	---------------------------	--

Mode	Config-VLAN Mode
-------------	------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	0
-----------------	---

Example	iss (config-vlan)# ip igmp snooping multicast-vlan profile 1
----------------	--



- Multicast snooping mode should be IP based.
- This command can be executed only after creating a multicast profile and setting the action for the created profile as permit.
- The configurations done by this command will take effect only if the profile is activated.

Related Command	<ul style="list-style-type: none"> • ip mcast profile – Creates or modifies a multicast profile. • permit– Configures the action for the profile as permit. • profile active – Activates the profile entry. • show ip mcast profile statistics – Displays the profile statistics.
------------------------	---

47.34 ip igmp snooping leavemode

This command configures the port leave mode for an interface. The mechanism to process the leave messages in the downstream is selected. The switch sends an IGMP query message to find if there are any host interested in the multicast group.

```
ip igmp snooping leavemode {exp-hosttrack | fastLeave | normalleave}
[InnerVlanId <short (1-4094)>]
```

Syntax Description	exp-hosttrack	-	Configures the port to use the explicit host tracking mode to process the leave messages. The decision to remove the interface is made based on the tracked host information
	fastLeave		Configures the port to use the fast leave mode to process the leave messages. On receiving a leave message the interface is removed from the group registration and the leave message is sent to the router ports.
	normalleave		Configures the port to use the normal leave mode. The normal leave mode is applicable only for v2 hosts. When the system receives a v2 leave message, it sends a group specific query on the interface. For v3 hosts normal leave has no effect.
	innerVlanId <short (1-4094)>]		Configures the inner vlan Id. In provider bridging domain, the customer vlan itag is denoted as innervlan id. This value ranges between 1 and 4094.
Mode	Interface configuration mode		
Package	Workgroup, Enterprise and Metro		
Defaults	exp-host track/fastLeave/normalleave	-	normalleave
Example	<pre>iss(config-if)# ip igmp snooping leavemode fastLeave InnerVlanId 1</pre>		



- The multicast forwarding mode has to be IP based
- The snooping system enhanced mode must be enabled.
- The leave process configuration level has to be port

**Related
Command**

- **snooping leave-process config-level** – Specifies the level of configuring the leave processing mechanisms
- **ip igmp snooping enhanced-mode** – Enables/disables snooping system enhanced mode in the switch.
- **show ip igmp snooping port-cfg** – Displays IGS Port configuration information for all Inner VLANs or a specific Inner VlanId or a given switch.
- **show ip igmp snooping multicast-receivers** – Displays IGMP multicast host information for all VLANs or a specific VLAN or specific VLAN and group address for a given switch or for all switches (if no switch is specified).

47.35 ip igmp snooping ratelimit

This command configures the rate limit for a downstream interface in units of the number of IGMP packets per second. The switch allows to configure the maximum rate of IGMP reports incoming for a port. The IGMP rate limiting eliminates the bursts or attacks from specific physical port. It prevents the exhaustion of system resources.

The no form of the command resets the rate limit to default value for an interface. By default, the rate limit will hold the maximum value supported by an unsigned integer and will not rate limit any IGMP packets.

```
ip igmp snooping ratelimit <integer> [InnerVlanId <short (1-4094)>]
```

```
no ip igmp snooping ratelimit [InnerVlanId <short (1-4094)>]
```

Syntax Description	InnerVlanId - Inner VLAN identifier. This value ranges between 1 and 4094.
---------------------------	---

Mode	Interface configuration mode
-------------	------------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	rate limit is 4294967295.
-----------------	---------------------------

Example	iss(config-if)# ip igmp snooping ratelimit 100 InnerVlanId 1
----------------	--



- The actual rate supported will depend on what the system can support.
- The snooping system enhanced mode must be enabled.
- The IGMP snooping filter must be enabled.

Related Command	<ul style="list-style-type: none"> • ip igmp snooping enhanced-mode – Enables/disables snooping system enhanced mode in the switch. • ip igmp snooping filter – Enables the IGMP snooping filter. • show ip igmp snooping port-cfg – Displays IGS Port configuration information for all Inner VLANs or a specific Inner VlanId or a given switch. • ip mcast profile – Creates or modifies a multicast profile. • profile active – Activates the profile entry.
------------------------	--

47.36 ip igmp snooping limit

This command configures the maximum limit type for an interface. The maximum limit is the number of unique registrations for a channel or group. The no form of the command configures the maximum limit type as none for an interface.

```
ip igmp snooping limit { channels | groups } <interger32> [InnerVlanId <short (1-4094)>]
```

```
no ip igmp snooping limit [InnerVlanId <short (1-4094)>]
```

Syntax Description	channels	- Configures the snooping maximum limit as channels (group, source). Channel limit is applied for IGMPv3 include and allow reports.
	groups	- Configures the snooping maximum limit as groups. Group limit is applied for all IGMP reports.
	InnerVlanId <short (1-4094)>	- Inner VLAN identifier. This value ranges between 1 and 4094.

Mode Interface configuration mode

Package Workgroup, Enterprise and Metro

Defaults The limit is set as none so that no limiting is done.

Example `iss(config-if)# ip igmp snooping limit groups 10 InnerVlanId 1`



The snooping system enhanced mode must be enabled.

- The IGMP snooping filter must be enabled.

Related Command

- **ip igmp snooping enhanced-mode** – Enables/disables snooping system enhanced mode in the switch.
- **ip igmp snooping filter** – Enables the IGMP snooping filter.
- **show ip igmp snooping port-cfg** – Displays IGS Port configuration information for all Inner VLANs or a specific Inner VlanId or a given switch.
- **ip mcast profile** – Creates or modifies a multicast profile.
- **profile active** – Activates the profile entry.

47.37 ip igmp snooping filter-profileId

This command configures the multicast profile index for a downstream interface. This profile contains a set of allowed or denied rules to be applied for the IGMP packets received through this downstream interface.

The no form of the command resets the multicast profile index to default value.

```
ip igmp snooping filter-profileId <integer> [InnerVlanId <short (1-4094)>]
```

```
no ip igmp snooping filter-profileId [InnerVlanId <short (1-4094)>]
```

Syntax Description	InnerVlanId <short (1-4094)>	- Configures the Inner VLAN identifier. This value ranges between 1 and 4094.
---------------------------	---	---

Mode	Interface configuration mode
-------------	------------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	The profile ID is 0.
-----------------	----------------------

Example	<pre>iss(config-if)# ip igmp snooping filter-profileId 2 InnerVlanId 1</pre>
----------------	--



- The snooping system enhanced mode must be enabled.
- The IGMP snooping filter must be enabled.

Related Command

- **ip igmp snooping enhanced-mode** – Enables/disables snooping system enhanced mode in the switch.
- **ip igmp snooping filter** – Enables the IGMP snooping filter.
- **snooping multicast-forwarding-mode ip** - Sets the snooping multicast forwarding mode as IP address based.
- **show ip igmp snooping port-cfg** – Displays IGS Port configuration information for all Inner VLANs or a specific Inner VlanId or a given switch.
- **ip mcast profile** – Creates or modifies a multicast profile.
- **profile active** – Activates the profile entry.
- **show ip mcast profile statistics** – Displays the profile statistics.

47.38 ip igmp snooping proxy

This command enables proxy in the IGMP snooping switch. In proxy mode, the switch acts as a querier for all downstream interfaces and a host for all upstream interfaces. The switch sends general query to all downstream interfaces at the query interval and collects information about the member ports. The proxy sends current consolidated report and state change report to upstream interfaces.

The no form of the command disables proxy in the IGMP snooping switch.

ip igmp snooping proxy

no ip igmp snooping proxy

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults The proxy is disabled in the IGMP snooping switch.

Example `iss(config)# ip igmp snooping proxy`



Proxy can be enabled in the IGMP snooping switch only if the proxy reporting is disabled in the snooping switch.

Related Command

- **no ip igmp snooping proxy-reporting** – Disables proxy reporting in the IGMP snooping switch.
- **show ip igmp snooping globals** – Displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switch (if switch is not specified).

47.39 ip igmp snooping max-response-code

This command sets the maximum response code inserted in general queries sent to host. The unit of the response code is tenth of second. This value ranges between 0 and 255.

The no form of the command sets the query response code to default value.

```
ip igmp snooping max-response-code <(0 - 255)>
```

```
no ip igmp snooping max-response-code
```

Mode	Config-VLAN Mode
-------------	------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	100
-----------------	-----

Example	iss(config-vlan)# ip igmp snooping max-response-code 10
----------------	---

Related Command	show ip igmp snooping - Displays IGMP snooping information for all VLANs or a specific VLAN.
------------------------	---

47.40 ip igmp snooping mrouter-port –time-out

This command configures the router port purge time-out interval for a VLAN. The time interval after which the proxy assumes there are no v1/v2 routers present on the upstream port. While the older querier timer is running, the proxy replies to all the queries with consolidated v1/v2 reports. When the timer expires, if the v2/v3 queriers are not present and the port is dynamically learnt, the port is purged. If the port is static, router port, the proxy replies to all queries with new version of v2/v3 consolidated reports.

The no form of the command resets the router port purge time-out interval to default, for a VLAN.

```
ip igmp snooping mrouter-port <ifXtype> <iface_list> time-out <short (60-600)>
```

```
no ip igmp snooping mrouter-port <interface-type> <0/a-b, 0/c, ...>
```

Syntax Description	<div> <div><ifXtype></div> <div>-</div> <div> <p>Configures the specified type of interface. The interface can be:</p> <p>fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</p> <p>gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</p> <p>extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</p> <p>i-lan – Internal LAN created on a bridge per IEEE 802.1ap.</p> <p>port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.</p> </div> </div>
	<div> <div><iface_list></div> <div>-</div> <div>Configures the interface list</div> </div>
	<div> <div>time-out <short (60-600)></div> <div>-</div> <div>Configures the router port purge time-out interval. This value ranges between 60 and 600 seconds.</div> </div>
	<div> <div><interface-type></div> <div>-</div> <div>Sets the interface type to be unconfigured.</div> </div>
	<div> <div><0/a-b, 0/c, ...></div> <div>-</div> <div>Sets the Interface list to be purged.</div> </div>
Mode	Config-VLAN Mode
Package	Workgroup, Enterprise and Metro

Defaults	time-out	- 125 seconds
-----------------	----------	---------------

Example	<pre>iss(config-vlan)# ip igmp snooping mrouter-port gigabitethernet 0/1-3 time-out 150</pre>
----------------	---



The router ports must be statically configured for the VLAN.

**Related
Command**


- **ip igmp snooping mrouter** – Configures statically the router ports for a VLAN
- **show ip igmp snooping mrouter detail**– Displays detailed information about the router ports.

47.41 ip igmp snooping mrouter-port-version

This command configures the operating version of IGMP PROXY on the upstream router port for a VLAN. The no form of the command resets the operating version of the IGMP PROXY on the upstream router port to its default operating version.

```
ip igmp snooping mrouter-port <ifXtype> <iface_list> version {v1 | v2 | v3}
```

```
no ip igmp snooping mrouter-port <ifXtype> <iface_list> version
```

Syntax Description	<div> <div><ifXtype></div> <div> <ul style="list-style-type: none"> - Configures the specified type of interface. The interface can be: </div> </div> <div> <div>fastethernet</div> <div>– Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.</div> </div> <div> <div>gigabitethernet</div> <div>– A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.</div> </div> <div> <div>extreme-ethernet</div> <div>– A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.</div> </div> <div> <div>i-lan / internal-lan</div> <div>– Internal LAN created on a bridge per IEEE 802.1ap.</div> </div> <div> <div>port-channel</div> <div>– Logical interface that represents an aggregator which contains several ports aggregated together.</div> </div>
	<div> <div><iface_list></div> <div> <ul style="list-style-type: none"> - Configures the interface list </div> </div>
	<div> <div>version</div> <div> <ul style="list-style-type: none"> - Configures the operating version of the IGMP snooping </div> </div> <div> <div>v1</div> <div>– IGMP snooping Version 1</div> </div> <div> <div>v2</div> <div>– IGMP snooping Version 2</div> </div> <div> <div>v3</div> <div>– IGMP snooping Version 3</div> </div>
Mode	Config-VLAN Mode
Package	Workgroup, Enterprise and Metro
Defaults	v3
Example	<pre>iss(config-vlan)# ip igmp snooping mrouter-port gigabitethernet 0/2 version v1</pre>
	The router ports must be statically configured for the VLAN.
Related Command	<ul style="list-style-type: none"> • ip igmp snooping mrouter – Configures statically the router ports for a VLAN. • show ip igmp snooping mrouter detail– Displays detailed information about the router ports

47.42 show ip igmp snooping mrouter

This command displays the router ports for all VLANs or a specific VLAN for a given switch or for all the switches (if no switch is specified). The interface details and the corresponding port number along with its type (static/dynamic) are displayed.

```
show ip igmp snooping mrouter [Vlan <vlan index>] [detail] [switch
<switch_name>]
```

Syntax Description	Vlan <vlan index>	- Displays the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
	detail	- Displays detailed information about the router ports
	switch <switch_name>	- Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Package Workgroup and Enterprise

Example Single Instance
iss# show ip igmp snooping mrouter

```
Vlan    Ports
-----  -----
      1  Gi0/1(dynamic), Gi0/2(static)
      2  Gi0/1(static), Gi0/2(dynamic)
```

Multiple Instance
iss# show ip igmp snooping mrouter
Switch cust1

```
Vlan    Ports
-----  -----
      1  Gi0/1(static)
      2  Gi0/1(static)
```

Switch cust2

```
Vlan    Ports
-----  -----
      1  Gi0/9(static)
      2  Gi0/9(static)
```

Related Command

- **ip igmp snooping mrouter-time-out / ip igmp querier-timeout**
- Sets the IGMP snooping router port purge time-out after which the port gets deleted, if no IGMP router control packets are received.

- `ip igmp snoop mrouter` - Configures statically the router ports for a VLAN.
- `ip igmp snoop mrouter-port -time-out` - Configures the router port purge time-out interval for a VLAN.
- `ip igmp snoop mrouter-port-version` - Configures the operating version of the router port for a VLAN.

47.43 show ip igmp snooping mrouter - Redundancy

This command displays the router ports for all VLANs or a specific VLAN for a given switch or for all switch (if no switch is specified).

```
show ip igmp snooping mrouter [Vlan <vlan index>] [redundancy] [detail]
[switch <switch_name>]
```

Syntax Description	Vlan <vlan index>	- Displays the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
	redundancy	- Displays the Synced Messages
	detail	- Displays detailed information about the router ports
	switch <switch_name>	- Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature..

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ip igmp snooping mrouter redundancy

```
Igs Redundancy Vlan Sync Data for Vlan 1
Vlan Router Port List
Vlan  Ports
-----
  1  Gi0/1(dynamic), Gi0/3(dynamic)

IGMP Router Port List
Vlan  IGMP Ports
-----
  1  Gi0/1(dynamic)
```

Related Command

- **ip igmp snooping mrouter** - Configures statically the router ports for a VLAN
- **ip igmp snooping mrouter-port -time-out** - Configures the router port purge time-out interval for a VLAN.
- **ip igmp snooping mrouter-port-version** - Configures the operating version of the router port for a VLAN.

47.44 show ip igmp snooping globals

This command displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switches (if switch is not specified).

```
show ip igmp snooping globals [switch <switch_name>]
```

Syntax **switch** - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

<switch_name>

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example Single Instance
 iss# show ip igmp snooping globals

Snooping Configuration

```
-----
IGMP Snooping globally enabled
IGMP Snooping is operationally enabled
IGMP Snooping Enhanced mode is disabled
Transmit Query on Topology Change globally disabled
Multicast forwarding mode is MAC based
Proxy globally disabled
Proxy reporting globally enabled
Filter is disabled
Router port purge interval is 125 seconds
Port purge interval is 260 seconds
Report forward interval is 5 seconds
Group specific query interval is 2 seconds
Reports are forwarded on router ports
Group specific query retry count is 2
Multicast VLAN disabled
Leave config level is Vlan based
```

Multiple Instance
 iss# show ip igmp snooping globals
 Switch default

Snooping Configuration

```
-----
IGMP Snooping globally enabled
IGMP Snooping is operationally enabled
IGMP Snooping Enhanced mode is disabled
Transmit Query on Topology Change globally disabled
Multicast forwarding mode is MAC based
Proxy globally disabled
```

```

Proxy reporting globally enabled
Filter is disabled
Router port purge interval is 125 seconds
Port purge interval is 260 seconds
Report forward interval is 5 seconds
Group specific query interval is 2 seconds
Reports are forwarded on router ports
Group specific query retry count is 2
Multicast VLAN disabled
Leave config level is Vlan based
  
```

**Related
Commands**

- **ip igmp snooping** - Enables IGMP snooping in the switch/a specific VLAN
- **ip igmp snooping proxy-reporting** - Enables proxy reporting in the IGMP snooping switch
- **snooping multicast-forwarding-mode** - Specifies the forwarding mode (IP based or MAC based) that will be effective on switch restart
- **ip igmp snooping mrouter-port -time-out / ip igmp querier-timeout** - Configures the router port purge time-out interval for a VLAN
- **ip igmp snooping port-purge-interval / ip igmp snooping source-only learning age-timer** - Sets the IGMP snooping port purge time interval after which the port gets deleted if no IGMP reports are received
- **ip igmp snooping report-suppression interval** - Sets the IGMP report-suppression interval
- **ip igmp snooping retry-count** - Sets the maximum number of group specific queries sent on a port on reception of a IGMPV2 leave message
- **ip igmp snooping version** - Specifies the IGMP snooping operating mode of the switch
- **ip igmp snooping fast-leave / ip igmp snooping vlan - immediate leave** - Enables fast leave processing for a specific VLAN
- **ip igmp snooping report-forward** - Specifies if IGMP reports must be forwarded on all ports or router ports of a VLAN
- **snooping leave-process config-level** - Specifies the level of configuring the leave processing mechanisms.
- **ip igmp snooping enhanced-mode** - Enables/disables snooping system enhanced mode in the switch.
- **ip igmp snooping multicast-vlan** - Enables/disables the multicast VLAN feature.
- **mvr** - Enables the multicast VLAN feature. This command is applicable only for the code using industry standard commands
- **ip igmp snooping filter** - Enables the IGMP snooping filter.
- **ip igmp snooping proxy** - Enables proxy in the IGMP snooping switch.

47.45 show ip igmp snooping

This command displays IGMP snooping information for all VLANs or a specific VLAN for a given context or for all the context (if no switch is specified).

```
show ip igmp snooping [Vlan <vlan id>] [switch <switch_name>]
```

Syntax Description	Vlan <vlan id>	- Displays the specified VLAN ID. This is a unique value that represents the specific VLAN created This value ranges between 1 and 4094.
	switch <switch_name>	- Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature..

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example Single Instance

```
iss# show ip igmp snooping vlan 2
```

Snooping VLAN Configuration for the VLAN 1

```
IGMP Snooping enabled
IGMP configured version is V3
Fast leave is disabled
Snooping switch is acting as Non-Querier
Query interval is 125 seconds
Port Purge Interval is 260 seconds
Max Response Code is 100, Time is 10 seconds
```

Multiple Instance

```
iss# show ip igmp snooping
```

```
Switch default
```

Snooping VLAN Configuration for the VLAN 1

```
IGMP Snooping enabled
IGMP configured version is V3
Fast leave is disabled
Snooping switch is configured as Querier
Snooping switch is acting as Non-Querier
Query interval is 125 seconds
Port Purge Interval is 260 seconds
Max Response Code is 100, Time is 10 seconds
```

**Related
Commands**

- **ip igmp snooping** - Enables IGMP snooping in the switch/a specific VLAN
- **ip igmp snooping version** - Specifies the IGMP snooping operating mode of switch
- **ip igmp snooping fast-leave / ip igmp snooping vlan - immediate leave** - Enables fast leave processing for a specific VLAN
- **ip igmp snooping querier** - Configures the IGMP snooping switch as a querier for a specific VLAN
- **ip igmp snooping query-interval** - Sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN
- **ip igmp snooping max-response-code** - Sets the maximum response code inserted in general queries send to host.

47.46 show ip igmp snooping - Redundancy

This command displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switch (if no switch is specified).

```
show ip igmp snooping [Vlan <vlan id>] [redundancy] [switch <switch_name>]
```

Syntax Description	Vlan <vlan id>	- Displays the specified VLAN ID. This is a unique value that represents the specific VLAN created This value ranges between 1 and 4094.
---------------------------	-----------------------------	---

redundancy	- Displays the Synced Messages
-------------------	--------------------------------

switch <switch_name>	- Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
-----------------------------------	--

Mode	Privileged EXEC Mode
-------------	----------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Example	iss# show ip igmp snooping redundancy
----------------	---------------------------------------

```
IGMP Snooping VLAN Configuration for VLAN 1
IGMP snooping switch is acting as Non-Querier
IGMP current operating version is V1
```

Related Commands	<ul style="list-style-type: none"> • ip igmp snooping - Enables IGMP snooping in the switch/a specific VLAN • ip igmp snooping version - Specifies the IGMP snooping operating mode of switch • ip igmp snooping fast-leave - Enables fast leave processing for a specific VLAN • ip igmp snooping querier - Configures the IGMP snooping switch as a querier for a specific VLAN • ip igmp snooping query-interval - Sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN
-------------------------	---

47.47 show ip igmp snooping groups

This command displays IGMP group information for all VLANs or a specific VLAN or specific VLAN and group address for a given switch or for all switch (if no switch is specified).

```
show ip igmp snooping groups [Vlan <vlan id> [Group <Address>]] [switch
<switch_name>]
```

Syntax Description	Vlan <vlan id>	- Displays the specified VLAN ID. This is a unique value that represents the specific VLAN created This value ranges between 1 and 4094.
	Group	- Displays the Group Address of the VLAN ID
	switch <switch_name>	- Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example Single Instance
/* IP based */
iss# show ip igmp snooping groups

```
IGMP Snooping Group information
-----
VLAN ID:2  Group Address: 227.1.1.1
Filter Mode: EXCLUDE
Exclude sources: None
V1/V2 Receiver Ports:
  Gi0/4
V3 Receiver Ports:
  Port Number: Gi0/2
    Include sources: None
    Exclude sources:
      12.0.0.10, 12.0.0.20
  Port Number: Gi0/3
    Include sources: None
    Exclude sources:
      12.0.0.40, 12.0.0.30
```

```
/* MAC based */
iss# show ip igmp snooping groups
```

```
IGMP Snooping Group information
-----
VLAN ID:2  Group Address: 227.1.1.1
Filter Mode: EXCLUDE
Exclude sources: None
Receiver Ports:
```

```
Gi0/2, Gi0/3, Gi0/4, Gi0/5

Multiple Instance
iss# show ip igmp snooping groups

Switch cust1

Snooping Group information
-----
VLAN ID:2   Group Address: 227.2.2.2
Filter Mode: EXCLUDE
Exclude sources: None
Receiver Ports:
    Gi0/3, Gi0/5, Gi0/6

Switch cust2

Snooping Group information
-----
VLAN ID:2   Group Address: 227.2.2.2
Filter Mode: EXCLUDE
Exclude sources: None
Receiver Ports:
    Gi0/10
```

**Related
Command**

ip igmp snooping - Enables IGMP snooping in the switch/a specific VLAN

47.48 show ip igmp snooping forwarding-database

This command displays multicast forwarding entries for all VLANs or a specific VLAN for a given switch or for all switch (if no switch is specified).

```
show ip igmp snooping forwarding-database [Vlan <vlan id>] [switch <switch_name>]
```

Syntax Description

Vlan <vlan id> - Displays the specified VLAN ID. This is a unique value that represents the specific VLAN created
This value ranges between 1 and 4094.

switch <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature..

Mode Privileged EXEC Mode

Package Workgroup and Enterprise

Example Single Instance

```
/* IP based */
iss# show ip igmp snooping forwarding-database
```

```
Vlan Source Address Group Address Ports
-----
2      12.0.0.10      227.1.1.1  Gi0/1, Gi0/3, Gi0/4
2      12.0.0.20      227.1.1.1  Gi0/1, Gi0/3, Gi0/4
2      12.0.0.30      227.1.1.1  Gi0/1, Gi0/2, Gi0/4
2      12.0.0.40      227.1.1.1  Gi0/1, Gi0/2, Gi0/
```

```
/* MAC based */
iss# show ip igmp snooping forwarding-database
```

```
Vlan MAC-Address Ports
-----
2 01:00:5e:01:01:01 Gi0/2, Gi0/3, Gi0/4, Gi0/5
2 01:00:5e:02:02:02 Gi0/2, Gi0/3
```

Multiple Instance

```
iss# show ip igmp snooping forwarding-database
```

```
Switch cust1
Vlan MAC-Address Ports
-----
2 01:00:5e:02:02:02 Gi0/2, Gi0/3, Gi0/5, Gi0/6
```

```
Switch cust2
Vlan  MAC-Address      Ports
----  -
      2  01:00:5e:02:02:02  Gi0/9, Gi0/10
```



IGS must be enabled in the switch prior to the execution of this command.

**Related
Command**

ip igmp snooping - Enables IGMP snooping in the switch/a specific
VLAN

47.49 show ip igmp snooping forwarding-database - Redundancy

This command displays multicast forwarding entries for all VLANs or a specific VLAN for a given switch or for all switch (if no switch is specified).

```
show ip igmp snooping forwarding-database [Vlan <vlan id>] [redundancy]
[switch <switch_name>]
```

Syntax Description

Vlan <vlan id> - Displays the specified VLAN ID. This is a unique value that represents the specific VLAN created
This value ranges between 1 and 4094.

Redundancy - Displays the Synced Messages.

switch <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ip igmp snooping forwarding-database redundancy

```
Igs Redundancy Multicast Group Info Sync Data
```

```
Vlan    Group Address  Ports
----    -
1       224.1.1.1      Gi0/2, Gi0/3
1       224.1.2.3      Gi0/1, Gi0/3
```



IGS must be enabled in the switch prior to the execution of this command.

Related Command **ip igmp snooping** - Enables IGMP snooping in the switch/a specific VLAN

47.50 show ip igmp snooping statistics

This command Displays IGMP snooping statistics for all VLANs or a specific VLAN for a given switch or for all switch (if no switch is specified).

show ip igmp snooping statistics [Vlan <vlan id>] [switch <switch_name>]

Syntax Description	Vlan <vlan id>	- Displays the specified VLAN ID. This is a unique value that represents the specific VLAN created This value ranges between 1 and 4094.
	switch <switch_name>	- Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode	

Package Workgroup, Enterprise and Metro

Example Single Instance
 iss# show ip igmp snooping statistics

```
IGMP Snooping Statistics for VLAN 1
IGMP Snooping General queries received : 3
IGMP Snooping Group specific queries received : 0
IGMP Snooping Group and source specific queries received : 0
IGMP Snooping V1/V2 reports received : 10
IGMP Snooping V3 reports received : 0
IGMP Snooping V3 IS_INCLUDE messages received : 0
IGMP Snooping V3 IS_EXCLUDE messages received : 0
IGMP Snooping V3 TO_INCLUDE messages received : 0
IGMP Snooping V3 TO_EXCLUDE messages received : 0
IGMP Snooping V3 ALLOW messages received : 0
IGMP Snooping V3 Block messages received : 0
IGMP Snooping V2 Leave messages received : 0
IGMP Snooping General queries transmitted : 0
IGMP Snooping Group specific queries transmitted : 2
IGMP Snooping V1/V2 reports transmitted : 0
IGMP Snooping V3 reports transmitted : 3
IGMP Snooping V2 leaves transmitted : 0
IGMP Snooping Packets dropped : 1
```

Multiple Instance
 iss# show ip igmp snooping statistics

```
Switch cust1
Snooping Statistics for VLAN 1
General queries received : 0
```

```
Group specific queries received : 0
Group and source specific queries received : 0
ASM reports received : 20
SSM reports received : 0
IS_INCLUDE messages received : 0
IS_EXCLUDE messages received : 0
TO_INCLUDE messages received : 0
TO_EXCLUDE messages received : 0
ALLOW messages received : 0
Block messages received : 0
Leave messages received : 0
General queries transmitted : 0
Group specific queries transmitted : 0
ASM reports transmitted : 1
SSM reports transmitted : 0
Leaves transmitted : 0
Packets dropped : 0

Snooping Statistics for VLAN 2
General queries received : 0
Group specific queries received : 0
Group and source specific queries received : 0
ASM reports received : 19
SSM reports received : 18
IS_INCLUDE messages received : 0
IS_EXCLUDE messages received : 0
TO_INCLUDE messages received : 0
TO_EXCLUDE messages received : 0
ALLOW messages received : 0
Block messages received : 0
Leave messages received : 0
General queries transmitted : 0
Group specific queries transmitted : 0
ASM reports transmitted : 2
SSM reports transmitted : 0
Leaves transmitted : 0
Packets dropped : 0

Switch cust2
Snooping Statistics for VLAN 1
General queries received : 0
Group specific queries received : 0
Group and source specific queries received : 0
ASM reports received : 0
SSM reports received : 0
IS_INCLUDE messages received : 0
IS_EXCLUDE messages received : 0
TO_INCLUDE messages received : 0
TO_EXCLUDE messages received : 0
ALLOW messages received : 0
Block messages received : 0
Leave messages received : 0
General queries transmitted : 0
Group specific queries transmitted : 0
ASM reports transmitted : 0
SSM reports transmitted : 0
Leaves transmitted : 0
```

Packets dropped : 0

Snooping Statistics for VLAN 2

General queries received : 0

Group specific queries received : 0

Group and source specific queries received : 0

ASM reports received : 0

SSM reports received : 0

IS_INCLUDE messages received : 0

IS_EXCLUDE messages received : 0

TO_INCLUDE messages received : 0

TO_EXCLUDE messages received : 0

ALLOW messages received : 0

Block messages received : 0

Leave messages received : 0

General queries transmitted : 0

Group specific queries transmitted : 0

ASM reports transmitted : 0

SSM reports transmitted : 0

Leaves transmitted : 0

Packets dropped : 0

**Related
Command**

ip igmp snooping - Enables IGMP snooping in the switch/a specific VLAN

47.51 show ip igmp snooping blocked-router

This command displays the blocked router ports for all VLANs or a specific VLAN for a given switch or for all the switches (if no switch is specified).

```
show ip igmp snooping blocked-router [Vlan <vlan index>] [switch
<switch_name>]
```

- | | |
|---------------------------|--|
| Syntax Description | Vlan <vlan index> - Displays the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.

switch <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. |
|---------------------------|--|

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example Single Instance
 iss# show ip igmp snooping blocked-router

```
Vlan  Ports
----  -
1     Gi0/1, Gi0/2, Gi0/3, Gi0/4
2     Gi0/6, Gi0/7, Gi0/8
```

Multiple Instance

iss# show ip igmp snooping blocked-router

Switch default

```
Vlan  Ports
----  -
1     Gi0/1
```

Switch cust

```
Vlan  Ports
----  -
1     Gi0/3
```

Related Command **ip igmp snooping blocked-router** – Configures statically the blocked router ports for a VLAN.

47.52 show ip igmp snooping multicast-receivers

This command displays IGMP multicast host information for all VLANs or a specific VLAN or specific VLAN and group address for a given switch or for all switches (if no switch is specified).

```
show ip igmp snooping multicast-receivers [Vlan <vlan id> [Group <Address>]]
[switch <switch_name>]
```

Syntax Description	Vlan <vlan id>	- Displays the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
	Group	- Displays the Multicast group address.
	switch <switch_name>	- Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example Single Instance
 iss# show ip igmp snooping multicast-receivers

Snooping Receiver Information

VLAN ID: 1 Group Address: 225.0.0.10
 Receiver Port: Gi0/2
 Attached Hosts: 12.0.0.10
 Exclude Sources: None

VLAN ID: 1 Group Address: 225.0.0.20
 Receiver Port: Gi0/2
 Attached Hosts: 12.0.0.20
 Include Sources: 14.0.0.10
 Receiver Port: Gi0/4
 Attached Hosts: 12.0.0.40
 Include Sources: 14.0.0.20

Multiple instance

iss# sh ip igmp snooping multicast-receivers

Snooping Receiver Information

Switch switch1

```
VLAN ID: 1 Group Address: 225.0.0.20
Receiver Port: Gi0/4
Attached Hosts: 12.0.0.30
Include Sources: 14.0.0.10
Attached Hosts: 12.0.0.40
Exclude Sources: None
```

```
Switch switch2
```

```
VLAN ID: 1 Group Address: 225.0.0.20
Receiver Port: Gi0/2
Attached Hosts: 12.0.0.10
Exclude Sources: None
Attached Hosts: 12.0.0.20
Include Sources: 14.0.0.10
```



- IGMP snooping must be enabled in the switch.
- The port leave mode for an interface must be set as **exp-hosttrack**

**Related
Command**

- **ip igmp snooping** - Enables IGMP snooping in the switch/a specific VLAN
- **ip igmp snooping leavemode exp-hosttrack** – Processes the leave messages using the explicit host tracking mechanism.

47.53 show ip igmp snooping port-cfg

This command displays IGS Port configuration information for all Inner VLANs or a specific Inner VlanId or a given switch.

```
show ip igmp snooping port-cfg [{interface <interface-type> <interface-id>
[InnerVlanId vlan-id(1-4094)] | switch <switch_name>}]
```

Syntax	interface	- Displays the interface type and interface identifier.
Description		The details to be provided are:
		<ul style="list-style-type: none"> • <interface-type> - Sets the type of interface. The interface can be: <ol style="list-style-type: none"> 1. fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second. 2. gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. 3. extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links. 4. i-lan – Internal LAN created on a bridge per IEEE 802.1ap. • <interface-id> - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan. Only i-lan ID is provided, for interface type i-lan.
	InnerVlanId	- Displays the Inner VLAN identifier. This value ranges between 1 and 4094.
	switch <switch_name>	- Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature..

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example Single Instance
 iss# show ip igmp snooping port-cfg

Snooping Port Configurations

Snooping Port Configuration for Port 2

Leave Process mode is Normal Leave

```
Rate limit on the interface is 100
Max limit Type is Groups
Max limit is 20
Current member count is 0
Profile Id is 0
```

```
Snooping Port Configuration for Port 3
Leave Process mode is Fast Leave
Rate limit on the interface is -1
Max limit Type is Channels
Max limit is 500
Current member count is 0
Profile Id is 0
```

```
iss# show ip igmp snooping port-cfg interface gigabitethernet
0/2
```

Snooping Port Configurations

```
-----
Snooping Port Configuration for Port 2
Leave Process mode is Normal Leave
Rate limit on the interface is 100
Max limit Type is Groups
Max limit is 20
Current member count is 0
Profile Id is 0
```

Multiple Instance

```
iss# show ip igmp snooping port-cfg
```

Snooping Port Configurations

```
-----
Snooping Port Configuration for Port 3
Leave Process mode is Fast Leave
Rate limit on the interface is 1000
Max limit Type is None
Max limit is 0
Current member count is 0
Profile Id is 0
```

```
Snooping Port Configuration for Port 4
Leave Process mode is Normal Leave
Rate limit on the interface is -1
Max limit Type is None
Max limit is 0
Current member count is 0
Profile Id is 1
Snooping Port Configuration for Port 6 and Inner Vlan Id 5
Leave Process mode is Normal Leave
Rate limit on the interface is 200
Max limit Type is None
Max limit is 0
Current member count is 0
Profile Id is 0
```

```
Snooping Port Configuration for Port 7 and Inner Vlan Id 0
Leave Process mode is Normal Leave
Rate limit on the interface is -1
Max limit Type is Channels
Max limit is 200
Current member count is 0
Profile Id is 1
```

```
Snooping Port Configuration for Port 7 and Inner Vlan Id 6
Leave Process mode is Normal Leave
Rate limit on the interface is -1
Max limit Type is Groups
Max limit is 100
Current member count is 0
Profile Id is 0
```

```
iss# show ip igmp snooping port-cfg interface gigabitethernet
0/7
```

Snooping Port Configurations

```
Switch switch1
Snooping Port Configuration for Port 7 and Inner Vlan Id 0
Leave Process mode is Normal Leave
Rate limit on the interface is -1
Max limit Type is Channels
Max limit is 200
Current member count is 0
Profile Id is 1
```

```
Snooping Port Configuration for Port 7 and Inner Vlan Id 6
Leave Process mode is Normal Leave
Rate limit on the interface is -1
Max limit Type is Groups
Max limit is 100
Current member count is 0
Profile Id is 0
```

```
iss# show ip igmp snooping port-cfg switch default
```

Snooping Port Configurations

```
Switch default
Snooping Port Configuration for Port 3
Leave Process mode is Fast Leave
Rate limit on the interface is 1000
Max limit Type is None
Max limit is 0
Current member count is 0
Profile Id is 0
```

```
Snooping Port Configuration for Port 4
Leave Process mode is Normal Leave
```

```
Rate limit on the interface is -1
Max limit Type is None
Max limit is 0
Current member count is 0
Profile Id is 1
```

**Related
Command**

- **ip igmp snooping leavemode** – Configures the port leave mode for an interface.
- **ip igmp snooping ratelimit** – Configures the rate limit for a downstream interface in units of the number of IGMP packets per second.
- **ip igmp snooping limit** – Configures the maximum limit type for an interface.
- **ip igmp snooping filter-profileId** – Configures the multicast profile index for a downstream interface.

47.54 show ip igmp snooping multicast-vlan

This command displays multicast VLAN statistics in a switch and displays various profiles mapped to the multicast VLANs.

show ip igmp snooping multicast-vlan [switch <switch_name>]

Syntax	switch	-	Displays the specified context. This value represents
Description	<switch_name>		unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example Single Instance

```
iss# show ip igmp snooping multicast-vlan
```

```
Multicast VLAN Statistics
```

```
=====
```

```
-----
```

```
Multicast VLAN disabled
```

```
Profile ID -- Multicast VLAN
```

```
----- -- -----
```

```
1      --      1
2      --      2
```

```
-----
```

Multiple Instance

```
iss# show ip igmp snooping multicast-vlan
```

```
Multicast VLAN Statistics
```

```
=====
```

```
-----
```

```
Multicast VLAN disabled
```

```
Profile ID -- Multicast VLAN
```

```
----- -- -----
```

```
1      --      1
```

```
-----
```

```
Switch cust
```

```
Multicast VLAN disabled
```

```
Profile ID -- Multicast VLAN
```

```
----- -- -----
```

```
1      --      1
```

```
-----
```


**Related
Command**

- **ip igmp snoopig multicast-vlan** – Enables/disables the multicast VLAN feature.
- **mvr** - Enables the multicast VLAN feature. This command is applicable only for the code using industry standard commands.

Chapter

48

MLD Snooping

MLD (Multicast Listener Discovery) is a protocol used by IPv6 router to discover the presence of multicast listeners (that is, nodes willing to receive multicast packets) on its direct links, and to discover specifically which multicast address is of interest to those neighboring nodes. It is used by applications to listen to some multicast group.

Interface Masters MLDS software is designed in accordance with the FSAP (Flexible Software Architecture for Portability) frame to ensure a high level of portability.



The list of CLI commands for the configuration of MLDS is common to both **Single Instance** and **Multiple Instance** except for a difference in the prompt that appears for the Switch with Multiple Instance support.

The prompt for the **Global Configuration Mode** is,

```
iss(config)#
```

The list of CLI commands for the configuration of MLDS is as follows:

- ipv6 mld snooping
- ipv6 mld snooping proxy-reporting
- ipv6 mld snooping mroutertime-out
- ipv6 mld snooping port-purge-interval
- ipv6 mld snooping report-suppression-interval
- ipv6 mld snooping retry-count
- ipv6 mld snooping group-query-interval
- ipv6 mld snooping report-forward

ISS

- ipv6 mld snooping version
- ipv6 mld snooping fast-leave
- ipv6 mld snooping querier
- ipv6 mld snooping query-interval
- ipv6 mld snooping mrouter
- debug ipv6 mld snooping
- show ipv6 mld snooping mrouter
- show ipv6 mld snooping globals
- show ipv6 mld snooping
- show ipv6 mld snooping groups
- show ipv6 mld snooping forwarding-database
- show ipv6 mld snooping statistics

48.1 ipv6 mld snooping

This command enables MLD snooping in the switch or a specific VLAN.

The no form of this command disables MLD snooping in the switch or a specific VLAN.

Memory resources required by the MLDS module are allocated and the module starts running. It initializes semaphore creation, timer task RBTtree, hash table, RBT Tree nodes MLD snooping is enabled and disabled globally in all the existing VLAN interfaces.

ipv6 mld snooping

no ipv6 mld snooping

Mode Global Configuration Mode/ Config-VLAN Mode

Package Workgroup, Enterprise and Metro

Defaults MLD snooping is globally disabled

Example

```
iss(config)# ipv6 mld snooping
iss(config-vlan)# ipv6 mld snooping
```



- GMRP has to be disabled for the MLDS to be enabled
- The MLDS can be enabled for a VLAN, only if the MLDS is started in the switch and the VLAN is activated.

Related Commands

- **set gmrp disabled** – Globally disables GMRP feature on all ports of a switch.
- **vlan active** - Activates a VLAN in the switch.
- **no shutdown snooping**- Starts the snooping in the switch
- **show ipv6 mld snooping globals** – Displays the global MLD snooping information
- **show ipv6 mld snooping** – Displays MLD snooping information for all VLANs or a specific VLAN
- **snooping multicast-forwarding-mode**– Specifies the snooping multicast forwarding mode

48.2 ipv6 mld snooping proxy-reporting

This command enables proxy reporting in the MLD snooping switch.

The no form of this command disables proxy reporting in the MLD snooping switch.

Configuring proxy-reporting summarizes the report sent by downstream hosts. It is used to build internal membership states and reduces MLD network traffic. When a query is received, it generates reports as consolidated bitmaps in the table and forwards it to the routers based on the available host information.

ipv6 mld snooping proxy-reporting

no ipv6 mld snooping proxy-reporting

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Proxy-reporting is enabled

Example `iss(config)# ipv6 mld snooping proxy-reporting`



Proxy reporting can be enabled in the MLD snooping switch only if the proxy is disabled in the switch.

Related Command `show ipv6 mld snooping globals` – Displays the global MLD snooping information.

48.3 ipv6 mld snooping mrouter-time-out

This command sets the MLD snooping router purge time-out after which the port gets deleted if no MLD router control packets are received. If the router control packet is received before the timer expiry, the timer is restarted. The no form of this command sets the MLD snooping router port purge time to default value. The value range for the time out is 60-600 seconds.

```
ipv6 mld snooping mrouter-time-out <(60-600) seconds>
```

```
no ipv6 mld snooping mrouter-time-out
```

Mode	Global Configuration Mode
-------------	---------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	125
-----------------	-----

Example	iss(config)# ipv6 mld snooping mrouter-time-out 75
----------------	--

Related Command	show ipv6 mld snooping globals – Displays the global MLD snooping information
------------------------	--

48.4 ipv6 mld snooping port-purge-interval

This command sets the MLD snooping port purge time interval after which the port gets deleted if MLD reports are not received.

The no form of this command sets the MLD snooping port purge time interval to default value. This value ranges between 130 and 1225.

For each port on which report has been received, this timer runs for the configured time. This timer is restarted whenever a report message is received from a host on the specific port. If the timer expires, then, the learnt port entry is purged from the multicast group.

```
ipv6 mld snooping port-purge-interval <(130-1225) seconds>
```

```
no ipv6 mld snooping port-purge-interval
```

Mode	Global Configuration Mode
-------------	---------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	260
-----------------	-----

Example	iss(config)# ipv6 mld snooping port-purge-interval 200
----------------	--

Related Command	<ul style="list-style-type: none">• show ipv6 mld snooping globals – Displays the MLD snooping information for all VLANs or a specific VLAN• show ipv6 mld snooping - Displays MLD snooping information for all VLANs or a specific VLAN
------------------------	---

48.5 ipv6 mld snooping report-suppression-interval

This command sets the MLD snooping report-suppression interval for which MLDv1 report messages do not get forwarded onto the router ports for the same group.

This value ranges is between 1 and 25. This timer is used when both proxy and proxy-reporting are disabled. This timer is started as soon as a report message for that group is forwarded out. Within this interval if another report for the same group arrives, it will not be forwarded.

The no form of this command sets the MLD snooping report-suppression interval to its default value.

```
ipv6 mld snooping report-suppression-interval <(1-25) seconds>
```

```
no ipv6 mld snooping report-suppression-interval
```

Mode	Global Configuration Mode
-------------	---------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	5
-----------------	---

Example	iss(config)# ipv6 mld snooping report-suppression-interval 20
----------------	---



This time interval is used when both proxy and proxy-reporting are disabled.

Related Command	show ipv6 mld snooping globals – Displays the global MLD snooping information
------------------------	--

48.6 ipv6 mld snooping retry-count

This command sets the maximum number of group specific queries sent on a port on the reception of MLDv1 leave message.

The no form of this command sets the maximum number of group specific queries sent on a port on the reception of leave message to its default value.

This value ranges between 1 and 5. When the switch receives leave message on a port, it sends group specific query to check if there are any interested receivers in the group. The Retry Count defines the maximum number of queries sent by the switch before deleting the port from the group membership information in the forwarding database. If the query count exceeds the limit, the port is deleted and the leave message is forwarded to the routers.

```
ipv6 mld snooping retry-count <1-5>
```

```
no ipv6 mld snooping retry-count
```

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	2
Example	iss(config)# ipv6 mld snooping retry-count 3
Related Command	show ipv6 mld snooping globals – Displays the global MLD snooping information

48.7 ipv6 mld snooping group-query-interval

This command configures the time interval that the switch waits for the membership reports from the interested receivers for the given multicast group after sending out query messages. This value ranges between 2 and 5. The no form of this command sets the group specific query interval time to its default value.

```
ipv6 mld snooping group-query-interval <(2-5) seconds>
```

```
no ipv6 mld snooping group-query-interval
```

Mode	Global Configuration Mode
-------------	---------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	2
-----------------	---

Example	iss(config)# ipv6 mld snooping group-query-interval 3
----------------	---

Related Commands	show ipv6 mld snooping globals – Displays the global MLD snooping information
-------------------------	--

48.8 ipv6 mld snooping report-forward

This command configures the MLD reports to be forwarded on all VLAN member ports or router ports. The no form of this command sets the MLD report-forwarding status to default value. This configuration is not valid in proxy or proxy-reporting mode.

```
ipv6 mld snooping report-forward {all-ports | router-ports}
```

```
no ipv6 mld snooping report-forward
```

Syntax Description	all-ports	- Configures the MLD reports to be forwarded on all the ports of a VLAN.
	router-ports	- Configures the MLD reports to be forwarded only on router ports of a VLAN.
Mode	Global Configuration Mode	
Package	Workgroup, Enterprise and Metro	
Defaults	router-ports	
Example	iss(config)# ipv6 mld snooping report-forward all-ports	
Related Command	show ipv6 mld snooping globals – Displays the global MLD snooping information	

48.9 ipv6 mld snooping version

This command configures the operating version of the MLD snooping switch for a specific VLAN.

ipv6 mld snooping version {v1 | v2}

Syntax Description	v1	- Configures the version as MLDv1. MLDS report is accessed only with group address. It is provided with leave request option.
	v2	- Configures the version as MLDv2. MLDS report is accessed with source and group address.

Mode Config-VLAN Mode

Package Workgroup, Enterprise and Metro

Defaults v2

Example `iss(config-vlan)#ipv6 mld snooping version v1`



- The configuration can be done only for the VLANs that are activated in the switch.

Related Command

- **vlan active**- Activates a VLAN in the switch.
- **show ipv6 mld snooping** – Displays MLD snooping information for all VLANs or a specific VLAN

48.10 **ipv6 mld snooping fast-leave**

This command configures fast leave processing for a specific VLAN. On receipt of a single leave message, the port information is immediately removed from the multicast group entry. The switch immediately removes the port from the forwarding table without sending a group specific query. The fast leave functionality does not verify if other interested receivers are still present for the multicast group on the same port. The no form of the command disables fast leave processing for a specific VLAN.

ipv6 mld snooping fast-leave

no ipv6 mld snooping fast-leave

Mode Config-VLAN Mode

Package Workgroup, Enterprise and Metro

Defaults Disabled

Example `iss(config-vlan)# ipv6 mld snooping fast-leave`



- The configuration can be done only for the VLANs that are activated in the switch.

**Related
Command**

- **vlan active** - Activates a VLAN in the switch.
- **show ipv6 mld snooping** - Displays MLD snooping information for all VLANs or a specific VLAN

48.11 ipv6 mld snooping querier

This command configures the MLD snooping switch as a querier for a specific VLAN. The no form of this command configures the MLD snooping switch as non-querier for a specific VLAN. The switch starts sending general queries at regular time intervals. When the router port gets operationally down and there are no router ports in the switch, the switch continues the querier functionality.

ipv6 mld snooping querier

no ipv6 mld snooping querier

Mode Config-VLAN Mode

Package Workgroup, Enterprise and Metro

Defaults Non-querier

Example `iss(config-vlan)# ipv6 mld snooping querier`



- The configuration can be done only for the VLANs that are activated in the switch.

Related Command

- **vlan active** - Activates a VLAN in the switch.
- **show ipv6 mld snooping** – Displays MLD snooping information for all VLANs or a specific VLAN

48.12 ipv6 mld snooping query-interval

This command sets the time period for which the switch waits after sending a group specific query to determine if the hosts are still interested in a specific multicast group. The no form of this command sets the MLDS query interval to default value. The value ranges between 60 and 600. In proxy reporting mode, general queries are sent on all downstream interfaces with this interval, only if the switch is the Querier.

```
ipv6 mld snooping query-interval <(60 - 600) seconds>
```

```
no ipv6 mld snooping query-interval
```

Mode Config-VLAN Mode

Package Workgroup, Enterprise and Metro

Defaults 125

Example `iss(config-vlan)# ipv6 mld snooping query-interval 65`



- The configuration can be done only for the VLANs that are activated in the switch.

Related Command

- **vlan active** - Activates a VLAN in the switch.
- **show ipv6 mld snooping** – Displays MLD snooping information for all VLANs or a specific VLAN

48.13 ipv6 mld snooping mrouter

This command configures statically the router ports for a VLAN. The no form of this command deletes the statically configured router ports for a VLAN. By default the router port list is set to none.

```
ipv6 mld snooping mrouter <interface-type> <0/a-b, 0/c, ...>
```

```
no ipv6 mld snooping mrouter <interface-type> <0/a-b, 0/c, ...>
```

Mode Config-VLAN Mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config-vlan)# ipv6 mld snooping mrouter gigabitethernet 0/1-3
```



- The configuration can be done only for the VLANs that are activated in the switch.
- The specified interface can be set as router ports for the VLAN, only if the interfaces are configured as member ports for that VLAN.

Related Command

- **vlan active** - Activates a VLAN in the switch.
- **ports** - Statically configures a VLAN entry with the required member ports, untagged ports and forbidden ports.
- **show ipv6 mld snooping mrouter** - Displays the router ports for all the VLANs or a specific VLAN.

48.14 debug ipv6 mld snooping

This command specifies the debug levels for MLD snooping module and the no form of the command resets the debug options for MLD snooping module.

```
debug    ipv6    mld    snooping    {[init][resources][tmr][src][grp][qry]
[vlan][pkt][fwd][mgmt] | all } [switch <switch_name>]
```

```
no debug    ipv6    mld    snooping    {[init][resources][tmr][src][grp][qry]
[vlan][pkt][fwd][mgmt] | all } [switch <switch_name>]
```

Syntax	init	- Generates Init and Shutdown trace messages at the instances when the module is initiated or shutdown. The information is logged in a file.
Description	resources	- Generates System Resources management trace messages when there is a change in the resource status. The information is logged in a file.
	tmr	- Generates Timer trace messages at the instances where timers are involved. The information is logged in a file.
	src	- Generates trace messages when Source Information is involved
	grp	- Generates trace messages when Group Information is involved.
	qry	- Generates trace messages for query related events.
	vlan	- Generates trace messages when VLAN related Information is involved
	pkt	- Generates packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets
	fwd	- Generates trace messages when forwarding database is involved.
	mgmt	- Generates debug statements for management plane functionality traces
	redundancy	- Generates debug statements for redundancy code flow traces. This trace is generated when there is a failure in redundancy processing

- | | |
|---------------|--|
| all | - Generates trace messages for all types of traces |
| switch | - Generates trace message when switch is involved. |

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Defaults Debugging is Disabled.

Example `iss# debug ipv6 mld snooping fwd`



- The MLDS debug can be enabled, only if the MLDS is started in the switch.

Related Command `show debugging` - Displays state of each debugging option

48.15 show ipv6 mld snooping mrouter

This command displays the router ports for all the VLANs or a specific VLAN. Interface, ports (type of ports) and switch details are displayed.

```
show ipv6 mld snooping mrouter [Vlan <vlan index>] [detail] [switch
<switch_name>]
```

Syntax Description	Vlan	- Displays the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
	detail	- Displays detailed information about the router ports.
	switch	- Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Example Single Instance
 iss# show ipv6 mld snooping mrouter Vlan 1

```
Vlan  Ports
----  -
1     Gi0/1(static)
```

Multiple Instance
 iss# show ipv6 mld snooping mrouter

Switch cust1

```
Vlan  Ports
----  -
2     Gi0/4(static)
```

Switch cust2

```
Vlan  Ports
----  -
1     Gi0/10(static)
2     Gi0/9(dynamic)
```

Related Command

- **ipv6 mld snooping mrouter** - Configures statically the router ports for a VLAN.

48.16 show ipv6 mld snooping globals

This command displays the global MLD snooping information for all VLANs or a specific VLAN. Information such as MLD Snooping globally enabled, MLD Snooping operationally enabled, Transmit Query on Topology Change and so on.

show ipv6 mld snooping globals [switch <switch_name>]

Syntax	switch	- Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
---------------	---------------	--

Mode	Privileged EXEC Mode
-------------	----------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Example	<pre>Single Instance iss# show ipv6 mld snooping globals Snooping Configuration ----- MLD Snooping globally enabled MLD Snooping is operationally enabled Transmit Query on Topology Change globally disabled Multicast forwarding mode is MAC based Proxy globally disabled Proxy reporting globally enabled Filter is disabled Router port purge interval is 125 seconds Port purge interval is 260 seconds Report forward interval is 5 seconds Group specific query interval is 2 seconds Reports are forwarded on router ports Queries are forwarded on non-router ports Group specific query retry count is 2 Multicast VLAN disabled Leave config level is Vlan based Report processing config level is on non-router ports Multiple Instance iss# show ipv6 mld snooping globals Switch default Snooping Configuration ----- MLD Snooping globally enabled MLD Snooping is operationally enabled Multicast forwarding mode is MAC based Proxy globally disabled</pre>
----------------	---

Proxy reporting globally enabled
Filter is disabled
Router port purge interval is 125 seconds
Port purge interval is 260 seconds
Report forward interval is 5 seconds
Group specific query interval is 2 seconds
Reports are forwarded on router ports
Queries are forwarded on non-router ports
Group specific query retry count is 2
Multicast VLAN disabled
Leave config level is Vlan based
Report processing config level is on non-router ports

**Related
Commands**

- **ipv6 mld snooping** - Enables MLD snooping in the switch
- **ipv6 mld snooping proxy-reporting** - Enables proxy reporting in the MLD snooping switch
- **snooping multicast-forwarding-mode** - Specifies the snooping multicast forwarding mode
- **ipv6 mld snooping mrouter-time-out** - Sets the MLD snooping router purge time-out after which the port gets deleted if no MLD router control packets are received
- **ipv6 mld snooping port-purge-interval** - Sets the MLD snooping port purge time interval after which the port gets deleted if MLD reports are not received
- **ipv6 mld snooping report-suppression-interval** - Sets the MLD snooping report-suppression time interval
- **ipv6 mld snooping retry-count** - Sets the maximum number of group specific queries sent on a port on the reception of MLDv1 done message
- **ipv6 mld snooping group-query-interval** - Configures the time interval that the switch waits for the membership reports from the interested receivers for the given multicast group after sending out query messages.
- **ipv6 mld snooping report-forward** - Specifies whether the MLD reports are forwarded on all VLAN member ports or router ports

48.17 show ipv6 mld snooping

This command displays MLD snooping information for all VLANs or a specific VLAN. Information such as MLD Snooping enabled, MLD configured version is v2 and so on.

```
show ipv6 mld snooping [Vlan <vlan id>] [switch <switch_name>]
```

Syntax Description	Vlan	- Displays the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
	switch	- Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
Single Instance
iss# show ipv6 mld snooping Vlan 1

Snooping VLAN Configuration for the VLAN 1
MLD Snooping enabled
MLD configured version is V2
Fast leave is disabled
Snooping switch is configured as Querier
Snooping switch is acting as Non-Querier
Startup Query Count is 2
Startup Query Interval is 31 seconds
Query interval is 125 seconds
Other Querier Present Interval is 255 seconds
Port Purge Interval is 157 seconds
Max Response Code is 10000, Time is 10 seconds

Multiple Instance
iss# show ipv6 mld snooping

Switch default

Snooping VLAN Configuration for the VLAN 1
MLD Snooping enabled
MLD configured version is V2
Fast leave is disabled
Snooping switch is configured as Querier
Snooping switch is acting as Non-Querier
Startup Query Count is 2
Startup Query Interval is 31 seconds
```

Query interval is 125 seconds
Other Querier Present Interval is 255 seconds
Port Purge Interval is 260 seconds
Max Response Code is 10000, Time is 10 seconds

**Related
Commands**

- **ipv6 mld snooping** – Enables MLD snooping in the switch
- **ipv6 mld snooping port-purge-interval** – Sets the MLD snooping port purge time interval after which the port gets deleted if MLD reports are not received
- **ipv6 mld snooping version** – Sets the operating version of the MLD snooping switch for a specific VLAN
- **ipv6 mld snooping fast-leave** - Enables fast leave processing for a specific VLAN
- **ipv6 mld snooping querier** – Configures the MLD snooping switch as a querier for a specific VLAN
- **ipv6 mld snooping query-interval** – Sets the time period with which the general queries are sent by the MLD snooping switch when it is configured as a querier on the VLAN
- **ip igmp snooping max-response-code** – Sets the maximum response code send in general queries.

48.18 show ipv6 mld snooping groups

This command displays the MLDS group information for all VLANs or a specific VLAN or a specific VLAN and group address. Information displayed in the output are Snooping Group information, VLAN id, Group address, Filter mode and so on.

```
show ipv6 mld snooping groups [Vlan <vlan id> [Group <Address>]] [switch
<string (32)>]
```

Syntax Description	Vlan	- Displays the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
	Group	- Group Address of the VLAN ID
	switch	- Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example Single Instance
iss# show ipv6 mld snooping groups

```
Snooping Group information
-----
VLAN ID:1  Group Address: ff07::1:1
Filter Mode: EXCLUDE
Exclude sources: None
ASM Receiver Ports:  Gi0/1
```

Multiple Instance
iss# show ipv6 mld snooping groups

```
Switch cust1

Snooping Group information
-----
VLAN ID:2  Group Address: ff02::1:1
Filter Mode: EXCLUDE
Exclude sources: None
Receiver Ports:
    Gi0/5

VLAN ID:2  Group Address: ff02::2:2
Filter Mode: EXCLUDE
Exclude sources: None
```

```
Receiver Ports:
  Gi0/5
```

```
Switch cust2
```

```
Snooping Group information
```

```
-----
VLAN ID:2  Group Address: ff02::1:1
Filter Mode: EXCLUDE
Exclude sources: None
Receiver Ports:
  Gi0/10
```

```
VLAN ID:2  Group Address: ff02::2:2
Filter Mode: EXCLUDE
Exclude sources: None
Receiver Ports:
  Gi0/11
```

**Related
Command**

ipv6 mld snooping - Enables MLD snooping in the switch

48.19 show ipv6 mld snooping forwarding-database

This command displays multicast forwarding entries for all VLANs or a specific VLAN. The information displayed are VLAN, Source address, Group address and Ports.

```
show ipv6 mld snooping forwarding-database [Vlan <vlan id>] [switch
<switch_name>]
```

Syntax Description

Vlan - Displays the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created.
This value ranges between 1 and 4094.

switch - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example Single Instance

```
/* IP based */
```

```
iss# show ipv6 mld snooping forwarding-database
```

Vlan	Source Address	Group Address	Ports
1	fe80::7	ff07::1:1	Gi0/1

```
/* MAC based */
```

```
iss# show ipv6 mld snooping forwarding-database
```

Vlan	MAC-Address	Ports
1	33:33:00:01:00:01	Gi0/1

Multiple Instance

```
iss# show ipv6 mld snooping forwarding-database
```

```
Switch cust1
```

Vlan	MAC-Address	Ports
2	33:33:00:01:00:01	Gi0/5
2	33:33:00:02:00:02	Gi0/5

```
Switch cust2
```

Related Command	Vlan	MAC-Address	Ports
	----	-----	-----
	2	33:33:00:01:00:01	Gi0/9, Gi0/10
	2	33:33:00:02:00:02	Gi0/9, Gi0/11
	ipv6 mld snooping - Enables MLD snooping in the switch		

48.20 show ipv6 mld snooping statistics

This command displays MLD snooping statistics for all VLANs or a specific VLAN. The information displayed are Snooping Statistics for VLAN 1, General queries received, Group specific queries received, Group and source specific queries received and so on.

show ipv6 mld snooping statistics [Vlan <vlan id>] [switch <string (32)>]

Syntax Description	Vlan	- Displays the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
	switch	- Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example Single Instance

```
iss# show ipv6 mld snooping statistics

Snooping Statistics for VLAN 1
  General queries received : 0
  Group specific queries received : 0
  Group and source specific queries received : 0
  ASM reports received : 1
  SSM reports received : 0
  IS_INCLUDE messages received : 0
  IS_EXCLUDE messages received : 0
  TO_INCLUDE messages received : 0
  TO_EXCLUDE messages received : 0
  ALLOW messages received : 0
  Block messages received : 0
  Done messages received : 0
  General queries transmitted : 0
  Group specific queries transmitted : 0
  Group and source specific queries transmitted : 0
  ASM reports transmitted : 0
  SSM reports transmitted : 0
  Done messages transmitted : 0
  Unsuccessful joins recieved count Per Vlan : 0
  Active/Successful joins recieved count Per Vlan: 0
  Active Groups count: 0
  Packets dropped : 0
```

Multiple Instance

```
iss# show ipv6 mld snooping statistics
```

```
Switch cust1
```

```
Snooping Statistics for VLAN 2
```

```
General queries received : 0
```

```
Group specific queries received : 0
```

```
Group and source specific queries received : 0
```

```
ASM reports received : 0
```

```
SSM reports received : 3
```

```
IS_INCLUDE messages received : 0
```

```
IS_EXCLUDE messages received : 0
```

```
TO_INCLUDE messages received : 0
```

```
TO_EXCLUDE messages received : 0
```

```
ALLOW messages received : 0
```

```
Block messages received : 0
```

```
Done messages received : 0
```

```
General queries transmitted : 2
```

```
Group specific queries transmitted : 0
```

```
ASM reports transmitted : 0
```

```
SSM reports transmitted : 0
```

```
Done messages transmitted : 0
```

```
Packets dropped : 0
```

```
Switch cust2
```

```
Snooping Statistics for VLAN 2
```

```
General queries received : 2
```

```
Group specific queries received : 0
```

```
Group and source specific queries received : 0
```

```
ASM reports received : 58
```

```
SSM reports received : 0
```

```
IS_INCLUDE messages received : 0
```

```
IS_EXCLUDE messages received : 0
```

```
TO_INCLUDE messages received : 0
```

```
TO_EXCLUDE messages received : 0
```

```
ALLOW messages received : 0
```

```
Block messages received : 0
```

```
Done messages received : 0
```

```
General queries transmitted : 0
```

```
Group specific queries transmitted : 0
```

```
ASM reports transmitted : 0
```

```
SSM reports transmitted : 3
```

```
Done messages transmitted : 0
```

```
Packets dropped : 0
```

**Related
Command**

ipv6 mld snooping – Enables MLD snooping in the switch

Chapter

49

IGMP

Interface Masters IGMP (Internet Group Management Protocol) is a portable implementation of the Internet Group Management Protocol Version 3. It implements the IGMP router functionalities required by the Multicast Routing Protocol.

Interface Masters IGMP confirms with RFC 3376 for IGMP v3 router functionality. **Interface Masters IGMP** supports the MIB defined in draft-ietf-magma-rfc2933-update-00.txt.

The deployment of the **Interface Masters IGMP** router can be within a routing domain that uses any Multicast Routing Protocol. **Interface Masters IGMP** informs MRPs about group membership messages and leave messages.

The list of CLI commands for the configuration of IGMP is as follows:

- set ip igmp
- ip igmp immediate-leave
- ip igmp version
- ip igmp query-interval
- ip igmp query-max-response-time
- ip igmp robustness
- ip igmp last-member-query-interval
- ip igmp static-group
- no ip igmp
- debug ip igmp

ISS

- show ip igmp global-config
- show ip igmp interface
- show ip igmp groups
- show ip igmp sources
- show ip igmp statistics

49.1 set ip igmp

This command enables or disables IGMP globally or on a particular interface.

```
set ip igmp {enable|disable}
```

**Syntax
Description**

- | | |
|----------------|-----------------|
| enable | - Enables IGMP |
| disable | - Disables IGMP |

Mode

Global Configuration Mode / Interface Configuration Mode

Package

Enterprise and Metro

Defaults

disable

Example

```
iss(config)# set ip igmp enable  
iss(config-if)# set ip igmp enable
```

**Related
Commands**

- **ip igmp proxy-service / ip igmp proxy service** - Enables IGMP Proxy service in the system
- **show ip igmp global-config** - Displays the global configuration of IGMP

49.2 ip igmp immediate-leave

This command enables immediate leave processing on the interface and the no form of the command disables immediate-leave processing.

ip igmp immediate-leave

no ip igmp immediate-leave

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults disable

Example `iss(config-if)# ip igmp immediate-leave`

**Related
Commands** • **show ip igmp interface** - Displays the interface configuration of IGMP

49.3 ip igmp version

This command sets the IGMP version on the interface and the no form of the command sets the default IGMP version on the interface.

```
ip igmp version { 1 | 2 | 3 }
```

```
no ip igmp version
```

Syntax	1 2 3	- IGMP versions
Description		

Mode	Interface Configuration Mode
-------------	------------------------------

Package	Enterprise and Metro
----------------	----------------------

Defaults	2
-----------------	---

Example	iss(config-if)# ip igmp version 1
----------------	-----------------------------------

Related Commands	<ul style="list-style-type: none">• show ip igmp interface - Displays the interface configuration of IGMP
-------------------------	--

49.4 ip igmp query-interval

This command sets the IGMP query interval for the interface and the no form of the command sets query-interval to the default value.

```
ip igmp query-interval <value (1-65535) seconds>
```

```
no ip igmp query-interval
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 125

Example `iss(config-if)# ip igmp query-interval 30`

**Related
Commands** • **show ip igmp interface** - Displays the interface configuration of IGMP

49.5 ip igmp query-max-response-time

This command sets the IGMP max query response value for the interface and the no form of the command sets the max query response to the default value.

```
ip igmp query-max-response-time <value (1-255) seconds>
```

```
no ip igmp query-max-response-time
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 100

Example iss(config-if)# ip igmp query-max-response-time 20

Related Commands

- **show ip igmp interface** - Displays the interface configuration of IGMP

49.6 ip igmp robustness

This command sets the IGMP robustness value for the interface and the no form of the command sets the robustness value to default value.

```
ip igmp robustness <value(1-255)>
```

```
no ip igmp robustness
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 2

Example iss(config-if)# ip igmp robustness 100

**Related
Commands** • **show ip igmp interface** - Displays the interface configuration of IGMP

49.7 ip igmp last-member-query-interval

This command sets the IGMP last member query interval for the interface and the no form of the command sets the last member query interval to the default value.

```
ip igmp last-member-query-interval <value(1-255)>
```

```
no ip igmp last-member-query-interval
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 10

Example `iss(config-if)# ip igmp last-member-query-interval 100`



- The **igmp version** on this interface must be set to 2.

**Related
Commands**

- **show ip igmp interface** - Displays the interface configuration of IGMP

49.8 ip igmp static-group

This command adds the static group membership on the interface and the no form of the command deletes the static group membership on the interface.

```
ip igmp static-group <Group Address> [source <Source Address>]
```

```
no ip igmp static-group <Group Address> [source <Source Address>]
```

Syntax Description	Group Address	- Group IP address
	source	- Source IP address

Mode Interface Configuration Mode

Package Enterprise and Metro

Example iss(config-if)# ip igmp static-group 224.1.2.3 source 12.0.0.1



- The **igmp version** on this interface must be set to 3 for configuring static group along with source information.

- Related Commands**
- **show ip igmp groups** - Displays the IGMP groups information
 - **show ip igmp sources** - Displays the IGMP sources information
 - **show ip igmp interface** - Displays the interface configuration of IGMP

49.9 no ip igmp

This command deletes the IGMP capable interface.

no ip igmp

Mode Interface Configuration Mode

Package Enterprise and Metro

Example `iss(config-if)# no ip igmp`



At least one of the interface configuration commands must have been executed to create the IGMP interface.

Related Commands

- **show ip igmp interface** - Displays the interface configuration of IGMP

49.10 debug ip igmp

This command enables the IGMP trace and the no form of the command disables the IGMP trace.

```
debug ip igmp { [i/o][grp][qry][tmr][mgmt] | [all] }
```

```
no debug ip igmp { [i/o][grp][qry][tmr][mgmt] | [all] }
```

Syntax Description	i/o	- Input/Output messages
	grp	- Group Related messages
	qry	- Query Related messages
	tmr	- Timer Related messages
	mgmt	- Management Configuration messages
	all	- All Traces

Mode Privileged EXEC Mode

Package Enterprise and Metro

Defaults Debugging is disabled.

Example iss# debug ip igmp all

49.11 show ip igmp global-config

This command displays the global configuration of IGMP.

```
show ip igmp global-config
```

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip igmp global-config
IGMP is globally enabled

Related Commands

- **set ip igmp** - Enables or disables IGMP
- **ip igmp proxy-service / ip igmp proxy service** - Enables IGMP Proxy service in the system

49.12 show ip igmp interface

This command displays the interface configuration of IGMP.

```
show ip igmp interface [{ Vlan <vlan-id> | <interface-type> <interface-id> }]
```

Syntax Description	Vlan	- VLAN ID
	interface-type	- Interface Type
	interface-id	- Interface Identifier

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip igmp interface

```
vlan1, line protocol is up
Internet Address is 10.0.0.1/8
IGMP is enabled on interface
Current IGMP router version is 2
IGMP query interval is 125 seconds
Last member query response interval is 10 seconds
IGMP max query response time is 100 seconds
Robustness value is 2
IGMP querying router is 10.0.0.1 (this system)
Fast leave is disabled on this interface
No multicast groups joined

vlan2, line protocol is up
Internet Address is 20.0.0.1/8
IGMP is enabled on interface
Current IGMP router version is 2
IGMP query interval is 125 seconds
Last member query response interval is 10 seconds
IGMP max query response time is 100 seconds
Robustness value is 2
IGMP querying router is 20.0.0.1 (this system)
Fast leave is disabled on this interface
No multicast groups joined
```

**Related
Commands**

- **ip igmp immediate-leave** - Enables immediate leave processing on the interface
- **ip igmp version** - Sets the IGMP version on the interface
- **ip igmp query-interval** - Sets the IGMP query interval for the interface
- **ip igmp query-max-response-time** - Sets the IGMP max query response value for the interface
- **ip igmp robustness** - Sets the IGMP robustness value for the interface
- **ip igmp last-member-query-interval** - Sets the IGMP last member query interval for the interface
- **no ip igmp** - Deletes the IGMP capable interface

49.13 show ip igmp groups

This command displays the IGMP groups information.

show ip igmp groups

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip igmp groups

I - Include Mode, E - Exclude Mode
S - Static Mbr, D - Dynamic Mbr

GroupAddress	Flg	Iface	UpTime	ExpiryTime	LastReporter
224.5.5.5	S	vlan2	[0d 00:00:22.28]	[0d 00:00:00.00]	20.0.0.1
226.7.7.7	IS	vlan3	[0d 00:00:04.59]	[0d 00:00:00.00]	30.0.0.1

Related Commands

- **ip igmp static-group** - Adds the static group membership on the interface

49.14 show ip igmp sources

This command displays the IGMP source information.

show ip igmp sources

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip igmp sources

I - Include Mode, E - Exclude Mode
S - Static Mbr, D - Dynamic Mbr
F - Forward List, N - Non-Forward List

GroupAddress	Iface	SrcAddress	Flg	ExpiryTime	LastReporter
226.7.7.7	vlan3	12.0.0.1	ISF	[0d 00:00:00.00]	30.0.0.1

Related Commands

- **ip igmp static-group** - Adds the static group membership on the interface

49.15 show ip igmp statistics

This command displays the IGMP statistics information.

```
show ip igmp statistics [{ Vlan <vlan-id> | <interface-type> <interface-id> }]
```

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip igmp statistics

```
IGMP Statistics for vlan1
  Number of General queries received 1
  Number of Group Specific queries received 0
  Number of Group and Source Specific queries received 0
  Number of v1/v2 reports received 0
  Number of v3 reports received 8
  Number of v2 leaves received 0
  Number of General queries transmitted 1
  Number of Group Specific queries transmitted 1
  Number of Group and Source Specific queries transmitted 2

IGMP Statistics for vlan3
  Number of General queries received 0
  Number of Group Specific queries received 0
  Number of Group and Source Specific queries received 0
  Number of v1/v2 reports received 0
  Number of v3 reports received 6
  Number of v2 leaves received 0
  Number of General queries transmitted 1
  Number of Group Specific queries transmitted 0
  Number of Group and Source Specific queries transmitted 0
```


Chapter

50

IGMP Proxy

IGMP Proxy (Internet Group Management Protocol Proxy) implementation is used to learn and proxy group membership information, and then forward multicast packets based on the learnt membership information. The IGMP Proxy learns membership information from IGMP hosts in downstream interfaces (interface to which hosts are connected) and substitutes (proxy) the information to upstream interface (interface to which upstream router is connected), based on the requirements of IGMP hosts.

IGMP Proxy is used mainly in edge devices. It reduces not only the cost of the devices, but also the operational overhead because, it does not need to support more complicated multicast routing protocols such as Protocol Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP).

The list of CLI commands for the configuration of IGMP is as follows:

- `ip igmp proxy-service / ip igmp proxy service`
- `ip igmp-proxy mrouter / ip igmp mroute proxy`
- `ip igmp-proxy mrouter-time-out`
- `ip igmp-proxy mrouter-version`
- `show ip igmp-proxy mrouter`
- `show ip igmp-proxy forwarding-database`

50.1 ip igmp proxy-service

This command enables IGMP Proxy service in the system. The no form of the command disables IGMP Proxy service in the system.

ip igmp proxy-service

no ip igmp proxy-service

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults IGMP proxy service is disabled.

Example `iss(config)# ip igmp proxy-service`



- IGMP module must be enabled globally.
- PIM and DVMRP modules must be disabled.

**Related
Commands**

- **set ip igmp** - Enables or disables IGMP
- **set ip dvmrp** – Enables / disables DVMRP in the switch
- **set ip pim** – Enables or disables PIM
- **ip multicast** - Enables PIM globally
- **show ip igmp global-config** - Displays the global configuration of IGMP

50.2 ip igmp proxy service

This command enables IGMP Proxy service in the system.

This command is a standardized implementation of the existing command; **ip igmp proxy-service**. It operates similar to the existing command.

ip igmp proxy service

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults IGMP proxy service is disabled.

Example `iss(config)# ip igmp proxy service`



- IGMP module must be enabled globally.
- PIM and DVMRP modules must be disabled.

**Related
Commands**

- **set ip igmp** - Enables or disables IGMP
- **set ip dvmrp** - Enables / disables DVMRP in the switch
- **set ip pim** - Enables or disables PIM
- **show ip igmp global-config** - Displays the global configuration of IGMP

50.3 ip igmp-proxy mrouter

This command configures the interface as an upstream interface. The no form of the command removes the interface from the upstream interface list.

```
ip igmp-proxy mrouter
```

```
no ip igmp-proxy mrouter
```

Mode Interface Configuration Mode
This command is applicable only in the VLAN interface mode.

Package Enterprise and Metro

Defaults The interface is configured as downstream interface.

Example `iss(config-if)# ip igmp-proxy mrouter`



IGMP must be enabled in the interface on which this configuration is executed.

Related Commands `show ip igmp-proxy mrouter` - Displays the upstream interface configuration of IGMP Proxy

50.4 ip igmp mroute proxy

This command configures the interface as an upstream interface.

This command is a standardized implementation of the existing command; **ip igmp-proxy mrouter**. It operates similar to the existing command.

ip igmp mroute proxy

Mode Interface Configuration Mode
This command is applicable only in the VLAN interface mode.

Package Enterprise and Metro

Defaults The interface is configured as downstream interface.

Example `iss(config-if)# ip igmp mroute proxy`



IGMP must be enabled in the interface on which this configuration is executed.

Related Commands **show ip igmp-proxy mrouter** - Displays the upstream interface configuration of IGMP Proxy

50.5 ip igmp-proxy mrouter-time-out

This command configures the upstream interface purge interval, after which the IGMP version on upstream interface will switch back to the configured version.

ip igmp-proxy mrouter-time-out <(60 - 600) seconds>

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 125

Example `iss(config-if)# ip igmp-proxy mrouter-time-out 100`



The interface, on which this configuration is executed, must be an upstream interface.

Related Commands `show ip igmp-proxy mrouter` - Displays the upstream interface configuration of IGMP Proxy

50.6 ip igmp-proxy mrouter-version

This command configures the version of IGMP on upstream interface.

```
ip igmp-proxy mrouter-version { 1 | 2 | 3 }
```

Syntax Description	1	- IGMP Version 1
	2	- IGMP Version 2
	3	- IGMP Version 3

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 3

Example `iss(config-if)# ip igmp-proxy mrouter-version 2`



The interface, on which this configuration is executed, must be an upstream interface.

Related Command `show ip igmp-proxy mrouter` - Displays the upstream interface configuration of IGMP Proxy

50.7 show ip igmp-proxy mrouter

This command displays the upstream interface configuration of IGMP Proxy.

show ip igmp-proxy mrouter [Vlan <vlan-id>]

Syntax Description **Vlan** - VLAN Interface

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip igmp-proxy mrouter

```

IfName/IfId  OperVersion  CfgVersion  UpTime/VersionExpiryTime  PurgeIntvl
-----
vlan3    /35      IGMPv3      IGMPv3      [0d 00:08:01.31]/0        125
vlan4    /36      IGMPv2      IGMPv2      [0d 00:00:25.67]/0        100

```

iss# show ip igmp-proxy mrouter vlan 4

```

IfName/IfId  OperVersion  CfgVersion  UpTime/VersionExpiryTime  PurgeIntvl
-----
vlan4    /36      IGMPv2      IGMPv2      [0d 00:00:48.40]/0        100

```



IGMP Proxy module must be enabled globally.

- Related Commands**
- **ip igmp-proxy mrouter / ip igmp mroute proxy** - Configures the interface as an upstream interface
 - **ip igmp-proxy mrouter-time-out** - Configures the upstream interface purge interval
 - **ip igmp-proxy mrouter-version** - Configures the version of IGMP on upstream interface

50.8 show ip igmp-proxy forwarding-database

This command displays the multicast forwarding information.

```
show ip igmp-proxy forwarding-database {[Vlan <vlan-id>] | [group group-  
address] | [source source-address]}
```

Syntax Description	Vlan	-	VLAN Interface
	group address	-	Multicast group address
	source address	-	Multicast source address

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip igmp-proxy forwarding-database

```
IGMP Proxy Multicast Routing table
-----
(Source, Group), Uptime/Expires(seconds)
Incoming Interface: Interface
Outgoing Interface:
Interface, State

(13.0.0.10, 234.0.0.3) , [0d 00:23:55.65]/ 26
Incoming Interface : vlan3
Outgoing InterfaceList :
vlan1, Forwarding
vlan4, Forwarding

(13.0.0.10, 234.0.0.4) , [0d 00:23:55.65]/ 13
Incoming Interface : vlan3
Outgoing InterfaceList :
vlan1, Forwarding
vlan2, Forwarding
vlan4, Forwarding

(13.0.0.11, 234.0.0.3) , [0d 00:23:55.65]/ 107
Incoming Interface : vlan3
Outgoing InterfaceList :
vlan2, Forwarding
vlan4, Forwarding
```

```
iss# show ip igmp-proxy forwarding-database group 234.0.0.4
```

```

IGMP Proxy Multicast Routing table
-----
(Source, Group) , Uptime/Expires(seconds)
Incoming Interface: Interface
Outgoing Interface:
Interface, State

(13.0.0.10, 234.0.0.4) , [0d 00:24:30.29]/ 77
  Incoming Interface : vlan3
  Outgoing InterfaceList :
    vlan1, Forwarding
    vlan2, Forwarding
    vlan4, Forwarding

```

```
iss# show ip igmp-proxy forwarding-database source 13.0.0.11
```

```

IGMP Proxy Multicast Routing table
-----
(Source, Group) , Uptime/Expires(seconds)
Incoming Interface: Interface
Outgoing Interface:
Interface, State

(13.0.0.11, 234.0.0.3) , [0d 00:24:49.36]/ 53
  Incoming Interface : vlan3
  Outgoing InterfaceList :
    vlan2, Forwarding
    vlan4, Forwarding

```



IGMP Proxy module must be enabled globally.

**Related
Command**

show ip igmp-proxy mrouter - Displays the upstream interface configuration of IGMP Proxy

Chapter

51

PIM

PIM (Protocol Independent Multicast) is a multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. Multicast IP Routing protocols are used to distribute data to multiple recipients. Using multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients. A multicast group identifies a set of recipients that are interested in a particular data stream, and is represented by an IP address from a well-defined range. Data sent to this IP address is forwarded to all members of the multicast group.

PIM is unicast routing protocol independent and can be operated in two modes: dense and sparse. It is designed to provide scalable inter-domain multicast routing across the Internet. PIM provides multicast routing and forwarding capability to the switch. It maintains the integrity of the hardware based multicast forwarding table with respect to the forwarding table existing in the software. It is independent of the underlying unicast routing protocol and uses the information from the Unicast Routing protocol.

The list of CLI commands for the configuration of PIM is as follows:

- `set ip pim / ip multicast`
- `ip pim version`
- `set ip pim threshold`
- `set ip pim spt-switchperiod`
- `set ip pim rp-threshold`
- `set ip pim rp-switchperiod`
- `set ip pim regstop-ratelimit-period`
- `set ip pim pmbr`
- `ip pim component`

- set ip pim static-rp
- set ip pim state-refresh origination-interval
- ip pim state-refresh disable
- set ip pim source-active interval
- set mode
- rp-candidate rp-address
- rp-candidate holdtime
- rp-static rp-address
- ip pim query-interval
- ip pim message-interval
- ip pim bsr-candidate - value / ip pim bsr-candidate – VLAN
- ip pim componentId
- ip pim dr-priority
- ip pim override-interval
- ip pim lan-delay
- set ip pim lan-prune-delay
- set ip pim graft-retry interval
- no ip pim interface
- debug ip pim
- show ip pim interface
- show ip pim neighbor
- show ip pim rp-candidate
- show ip pim rp-set
- show ip pim bsr
- show ip pim rp-static
- show ip pim component
- show ip pim thresholds
- show ip pim mroute
- show ip pim redundancy state
- show ip pim redundancy shadow-table

51.1 set ip pim

This command enables or disables PIM globally.

```
set ip pim { enable | disable }
```

Syntax Description	enable	- Enables PIM
	disable	- Disables PIM

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults Disable

Example iss (config)# set ip pim enable



- PIM mode will be set as sparse, when PIM is enabled globally.
- IGMP proxy service must be disabled in the system, before enabling the PIM globally.

Related Command

- **no ip igmp proxy-service** - Disables IGMP Proxy service in the system
- **show ip pim interface** – Displays the routers PIM interfaces

51.2 ip multicast

This command enables PIM globally.

This command is a standardized implementation of the existing command; **set ip pim**. It operates similar to the existing command.

ip multicast

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults PIM is disabled.

Example `iss (config)# ip multicast`



- PIM mode will be set as sparse, when PIM is enabled globally.
- IGMP proxy service must be disabled in the system, before enabling the PIM globally.

Related Command

- **no ip igmp proxy-service** - Disables IGMP Proxy service in the system
- **show ip pim interface** – Displays the routers PIM interfaces

51.3 ip pim version

This command sets the PIM version.

```
ip pim version { 1 | 2 }
```

Syntax	1 2	-	PIM version is configured either as v1 or v2.
Description			Only PIM version 2 is currently supported.

Mode	Global Configuration Mode
-------------	---------------------------

Package	Enterprise and Metro
----------------	----------------------

Example	iss (config)# ip pim version 2
----------------	--------------------------------

51.4 set ip pim threshold

This command specifies the SPT group or source threshold when exceeded, switching to shortest path tree is initiated. To switch to SPT, the threshold MUST be configured.

```
set ip pim threshold { spt-grp | spt-src } < number of packets (0-2147483647) >
```

Syntax Description	spt-grp	- The threshold of data rate for any group when exceeded, source specific counters are initiated for that particular group. It is based on number of bits per second.
	spt-src	- The switching to Shortest Path Tree is initiated, when the threshold of data rate for any source is exceeded. It is based on number of bits per second.
	number of packets	- Number of packets
Mode	Global Configuration Mode	
Package	Enterprise and Metro	
Defaults	0	
Example	iss (config)# set ip pim threshold spt-grp 50	
Related Command	show ip pim thresholds – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM	

51.5 set ip pim spt-switchperiod

This command specifies the period (in seconds) over which the data rate is to be monitored for switching to shortest path tree.

set ip pim spt-switchperiod <0-2147483647(in secs)>

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults 0

Example `iss (config)# set ip pim spt-switchperiod 60`



- The same period is used for monitoring the data rate for both source and group. To switch to SPT, this period must be configured.
- The SPT (Shortest Path Tree) is used for multicast transmission of packets with the shortest path from sender to recipients

Related Command **show ip pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM

51.6 set ip pim rp-threshold

This command specifies the threshold at which the RP (Rendezvous Point) initiates switching to source specific shortest path tree.

```
set ip pim rp-threshold <0-2147483647(number of reg packets)>
```

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults 0

Example `iss (config)# set ip pim rp-threshold 50`



To switch to SPT, this threshold must be configured and this switching is based on the number of registered packets received.

Related Command **show ip pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM

51.7 set ip pim rp-switchperiod

This command specifies the period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree.

set ip pim rp-switchperiod <0-2147483647(in secs)>

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults 0

Example `iss (config)# set ip pim rp- switchperiod 100`



- To switch to SPT, this period must be configured
- RP-tree is a pattern that multicast packets are sent to a PIM-SM router by unicast and then forwarded to actual recipients from RP

Related Command **show ip pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM

51.8 set ip pim regstop-ratelimit-period

This command specifies the period over which RP monitors the number of register packets after sending the register stop message.

```
set ip pim regstop-ratelimit-period <0-2147483647(in secs)>
```

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults 5

Example `iss (config)# set ip pim regstop-ratelimit-period 100`



Register stop message is used to avoid encapsulation of multicast data packets from the first hop router to the RP.

Related Command `show ip pim thresholds` – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM

51.9 set ip pim pmbr

This command enables or disables the PMBR (PIM Multicast Border Router) Status.

```
set ip pim pmbr { enable | disable }
```

Syntax Description	enable	- Enables the PMBR Status
	disable	- Disables the PMBR Status

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults disable

Example `iss (config)# set ip pim pmbr enable`



- A PMBR integrates two different PIM domains (either PIM -SM or PIM -DM)
- A PMBR connects a PIM domain to other multicast routing domain(s)

Related Command `show ip pim thresholds` – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM

51.10 ip pim component

This command configures the PIM component in the router and the no form of the command destroys the PIM component.

```
ip pim component <ComponentId (1-255)>
```

```
no ip pim component <ComponentId (2-255)>
```

Mode Global Configuration Mode

Package Enterprise and Metro

Example iss (config)# ip pim component 1



- The PIM Component 1 cannot be deleted as it is the default component.
- The PIM Component corresponds to each instance of a PIM domain and classifies it as Sparse or Dense mode.

Related Command `show ip pim component` - Displays the component information

51.11 set ip pim static-rp

This command enables or disables the Static RP configuration Status. This command specifies whether to use the configured static- RP.

```
set ip pim static-rp { enable | disable }
```

Syntax Description	enable	- Enables the Static RP configuration Status
---------------------------	---------------	--

	disable	- Disables the Static RP configuration Status
--	----------------	---

Mode	Global Configuration Mode
-------------	---------------------------

Package	Enterprise and Metro
----------------	----------------------

Defaults	disable
-----------------	---------

Example	iss (config)# set ip pim static-rp enable
----------------	---

Related Commands	<ul style="list-style-type: none">• show ip pim rp-set – Displays the RP-set information• show ip pim rp-static – Displays the RP-static information
-------------------------	---

51.12 set ip pim state-refresh origination-interval

This command sets the interval between successive SRM (State Refresh Messages) control messages originated and sent out by the router. The no form of the command disables origination (generation) of SRM control messages by the router.

```
set ip pim state-refresh origination-interval [<4-100>]
```

```
no ip pim state-refresh origination-interval
```

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults 60 seconds

Example `iss(config)# set ip pim state-refresh origination-interval 50`



This command is useful if the router is the First-hop router. That is, the source is directly connected.

This command will be used only if the pim mode is dense.

Related Command `show ip pim interface detail` - Displays the router's PIM interfaces.

51.13 ip pim state-refresh disable

This command disables the SRM processing and forwarding, that is, the router drops the State Refresh Messages, if received and also the router will not advertise the SR Capability in Hello messages.. The no form of the command enables the SRM processing and forwarding. On enabling, this router advertises itself as SR Capable in Hello Messages.

ip pim state-refresh disable

no ip pim state-refresh disable

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults SRM processing and forwarding is enabled.

Example `iss(config)# ip pim state-refresh disable`



This command will be used only if the pim mode is dense.

Related Command **show ip pim interface detail** - Displays the router's PIM interfaces.

51.14 set ip pim source-active interval

This command sets the time duration for which the SRM control messages would be originated by the router after a data packet is received. The no form of the command sets the source active interval to the default value.

```
set ip pim source-active interval <120-210>
```

```
no ip pim source-active interval
```

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults 210 seconds

Example `iss(config)# set ip pim source-active interval 150`



This command is useful if the router is the First-hop router. That is, the source is directly connected.

This command will be used only if the pim mode is dense.

Related Command `show ip pim mroute` - Displays the PIM multicast information.

51.15 set mode

This command sets the component mode to sparse or dense.

```
set mode {sparse | dense}
```

Syntax Description	sparse	- Sparse mode
---------------------------	---------------	---------------

	dense	- Dense mode
--	--------------	--------------

Mode	PIM Component Mode
-------------	--------------------

Package	Enterprise and Metro
----------------	----------------------

Defaults	sparse
-----------------	--------

Example	<code>iss(pim-comp)# set mode dense</code>
----------------	--



- Sparse-mode routing protocols use shared trees. In a shared tree, sources forward multicast datagrams to a directly connected router, the designated router. The designated router encapsulates the datagram and unicasts it to an assigned RP router, which then forwards the datagram to members of multicast groups
- Dense mode protocols are data driven, where multicast sources starts sending multicast data packets and receivers join if they want data packets or prune themselves

Related Command	<code>show ip pim component</code> – Displays the component information
------------------------	---

51.16 rp-candidate rp-address

This command sets the address of the interface, which will be advertised as a Candidate-RP and the no form of the command disables the address of the interface, which will be advertised as a Candidate-RP.

```
rp-candidate rp-address <Group Address> <Group Mask> <IP address> [Priority <0-255>]
```

```
no rp-candidate rp-address <Group Address> <Group Mask> <RP address>
```

Syntax Description	Group Address	- The IP multicast group address for which this entry contains multicast routing information
	Group Mask	- The IP multicast group address mask that, gives the group prefix for which this entry contains information about the RP
	IP address	- IP address
	Priority <0-255>	- Sets the priority of the candidate RP. This value ranges between 0 and 255.

Mode PIM Component Mode

Package Enterprise and Metro

Example

```
iss(pim-comp)# rp-candidate rp-address 224.1.0.0 255.255.0.0 20.0.0.2
```



A Candidate-RP is a router configured to send periodic Candidate-RP-Advertisement messages to the BSR, and processes Join/Prune or Register messages for the advertised group prefix, when it is elected as a RP.

Related Commands

- **show ip pim rp-set** – Displays the RP-set information
- **show ip pim rp-candidate** – Displays the RP-candidate information

51.17 rp-candidate holdtime

This command sets the holdtime of the component when it is a candidate RP in the local domain and the no form of the command sets the default holdtime (0) of the component.

```
rp-candidate holdtime <Holdtime value (0-255)>
```

```
no rp-candidate holdtime
```

Mode PIM Component Mode

Package Enterprise and Metro

Defaults 0

Example `iss(pim-comp)# rp-candidate holdtime 25`



- If its value is set to 0, it indicates that the local system is not a candidate RP
- Holdtime is the amount of time the candidate RP advertisement is valid. This field allows advertisements to be aged out

Related Command `show ip pim rp-candidate` – Displays the RP-candidate information

51.18 rp-static rp-address

This command sets the address of the interface, which will be advertised as a Static-RP and the no form of the command disables the address of the interface, which will be advertised as a Static-RP.

```
rp-static rp-address <Group Address> <Group Mask> <IP address>
```

```
no rp-static rp-address <Group Address> <Group Mask>
```

Syntax Description	Group Address	- Indicates the PIM Sparse multicast group address using the listed RP.
---------------------------	----------------------	---

Group Mask	- The IP multicast group address mask that gives the group prefix for which this entry contains information about the RP
-------------------	--

IP address	- IP address
-------------------	--------------

Mode	PIM Component Mode
-------------	--------------------

Package	Enterprise and Metro
----------------	----------------------

Example	<pre>iss(pim-comp)# rp-static rp-address 224.1.0.0 255.255.0.0 20.0.0.2</pre>
----------------	---



Static configuration allows additional structuring of the multicast traffic by directing the multicast join/prune messages to statically configured RPs.

Related Commands	show ip pim rp-static – Displays the RP-static information
-------------------------	---

51.19 ip pim query-interval

This command sets the frequency at which PIM hello messages are transmitted on this interface and the no form of the command sets the default hello timer interval for this interface.

```
ip pim query-interval <Interval (0-65535) secs>
```

```
no ip pim query-interval
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 30

Example `iss (config-if)# ip pim query-interval 60`



The query message informs the presence of a PIM router on the interface to the neighboring PIM routers.

Related Command `show ip pim interface` – Displays the routers PIM interfaces

51.20 ip pim message-interval

This command sets the frequency at which PIM Join/Prune messages are transmitted on this PIM interface and the no form of the command sets the default value for PIM Join/Prune message.

```
ip pim message-interval <Interval (0-65535)>
```

```
no ip pim message-interval
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 60

Example iss (config-if)# ip pim message-interval 120



The same Join/Prune message interval must be used on all the PIM routers in the PIM domain. If all the routers do not use the same timer interval, the performance of PIM Sparse can be adversely affected.

Related Command **show ip pim interface** – Displays the routers PIM interfaces

51.21 ip pim bsr-candidate - value

This command sets the preference value for the local interface as a candidate bootstrap router and the no form of the command sets the default preference value for the local interface as a candidate bootstrap router.

```
ip pim bsr-candidate <value (0-255)>
```

```
no ip pim bsr-candidate
```

Mode Interface Configuration Mode
This command is applicable only in the VLAN interface mode.

Package Enterprise and Metro

Defaults 0

Example iss (config-if)# ip pim bsr-candidate 1



A BSR is a dynamically elected router within a PIM domain

Related Command **show ip pim bsr** – Displays the BSR information

51.22 ip pim bsr-candidate – VLAN

This command sets the local interface as a candidate BSR (Bootstrap Router).

This command is a standardized implementation of the existing command; **ip pim bsr-candidate -value**. It operates similar to the existing command.

```
ip pim bsr-candidate <vlan-interface-no (0-255)> [<hash-mask-length>][priority <value>]
```

Syntax Description	vlan-interface-no	-	VLAN interface number from which BSR address is derived to make BSR as a candidate. This value ranges between 0 and 255.
	hash-mask-length		Length (in bits) of the mask that is to be ANDed with the group address before calling the hash function. This value ranges between 0 and 32. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
	priority		Priority of the candidate BSR. This value ranges between 0 and 255.

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults

hash-mask-length	-	30
priority	-	0

Example `iss(config)# ip pim bsr-candidate 1 priority 100`



The router with highest priority is considered as the BSR. If the priority values are same, then the router with largest IP address is considered as the BSR.

Related Commands `show ip pim bsr` – Displays the BSR information

51.23 ip pim componentId

This command adds the interface to the component.

ip pim componentId <value(1-255)>

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 1

Example `iss (config-if)# ip pim componentId 1`



This command adds the current VLAN into the specified PIM component.

**Related
Commands**

- **ip pim component** – Configures the PIM component in the router
- **show ip pim component** – Displays the component information

51.24 ip pim dr-priority

This command sets the designated router priority value configured for the router interface and the no form of the command sets the default designated router priority value (0) for the router interface.

```
ip pim dr-priority <priority(1-65535)>
```

```
no ip pim dr-priority
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 1

Example iss (config-if)# ip pim dr-priority 100



The DR sets up multicast route entries and sends corresponding Join/Prune and Register messages on behalf of directly-connected receivers and sources, respectively.

Related Command **show ip pim interface** – Displays the routers PIM interfaces

51.25 ip pim override-interval

This command sets the override interval configured for router interface and the no form of the command sets the default override interval (0) for router interface.

```
ip pim override-interval <interval (0-65535)>
```

```
no ip pim override-interval
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 0

Example iss (config-if)# ip pim override-interval 100



Override interval is the random amount of time delayed for sending override messages to avoid synchronization of override messages when multiple downstream routers share a multi-access link.

Related Command **show ip pim interface** – Displays the routers PIM interfaces

51.26 ip pim lan-delay

This command sets the LanDelay configured for the router interface and the no form of the command sets the default LanDelay (0) for the router per interface.

```
ip pim lan-delay <value(0-65535)>
```

```
no ip pim lan-delay
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 0

Example iss (config-if)# ip pim lan-delay 120



The LAN Delay inserted by a router in the LAN Prune Delay option expresses the expected message propagation delay on the interface. It is used by upstream routers to find out the delayed time interval for a Join override message before pruning an interface.

Related Command **show ip pim interface** – Displays the routers PIM interfaces

51.27 set ip pim lan-prune-delay

This command sets the LanPruneDelay bit configured for the router interface to advertise the Lan delay.

```
set ip pim lan-prune-delay { enable | disable }
```

Syntax Description	enable	- Enables LAN-prune-delay
---------------------------	---------------	---------------------------

	disable	- Disables LAN-prune-delay
--	----------------	----------------------------

Mode	Interface Configuration Mode
-------------	------------------------------

Package	Enterprise and Metro
----------------	----------------------

Defaults	disable
-----------------	---------

Example	iss (config-if)# ip pim lan-prune-delay enable
----------------	--



The command specifies whether to use LAN prune delay or not.

Related Command	show ip pim interface – Displays the routers PIM interfaces
------------------------	--

51.28 set ip pim graft-retry interval

This command sets the time before which graft is retransmitted upon no receipt of Graft ACK. The no form of the command sets the graft retry interval to the default value.

```
set ip pim graft-retry interval <value(1-10)>
```

```
no ip pim graft-retry interval
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 3 seconds

Example iss(config-if)# set ip pim graft-retry interval 4

Related Command **show ip pim interface detail** - Displays the router's PIM interfaces.

51.29 **no ip pim interface**

This command deletes an interface at PIM level.

no ip pim interface

Mode Interface Configuration Mode

Package Enterprise and Metro

Example iss (config-if)# no ip pim interface



This command is used to destroy the interface at PIM.

Related Command **show ip pim interface** – Displays the routers PIM interfaces

51.30 debug ip pim

This command enables PIM trace and the no form of the command disables PIM trace.

```
debug ip pim {[nbr][grp][jp][ast][bsr][io][pmbr][mrt][mdh][mgmt][srm][red] | [all]}
```

```
no debug ip pim {[nbr][grp][jp][ast][bsr][io][pmbr][mrt][mdh][mgmt][srm][red] | [all]}
```

Syntax Description	nbr	- Neighbor Discovery traces
	grp	- Group Membership traces
	jp	- Join or Prune traces
	ast	- Assert state traces
	bsr	- Bootstrap/RP traces
	io	- Input Output traces
	pmbr	- Interoperability traces
	mrt	- Multicast Route Table Update traces
	mdh	- Multicast Data Handling traces
	mgmt	- Configuration traces
	srm	- State Refresh Messages
	red	- Redundancy traces
	all	- All traces

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss # debug ip pim all



A Four byte integer value is specified for enabling the level of debugging. Each bit in the four byte integer variable represents a level of debugging. The combinations of levels are also allowed. The user has to enter the corresponding integer value for the bit set.

Related Command **show ip pim interface** – Displays the routers PIM interfaces

51.31 show ip pim interface

This command displays the router's PIM interfaces.

```
show ip pim interface [{ Vlan <vlan-id> | <interface-type> <interface-id> | detail }]
```

Syntax Description	Vlan	- VLAN ID
	detail	- Detailed information of the interface
	interface-type	- Interface Type
	interface-id	- Interface Identifier

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example

```
iss# show ip pim interface

Address IfName/IfId Ver/Mode Nbr   Qry    DR-Address DR-Prio
                        Count Interval
10.0.0.1  vlan1/160 2/Sparse   0    45    10.0.0.1    5
20.0.0.1  vlan2/33 2/Sparse   0    30    20.0.0.1    1
30.0.0.1  vlan3/34 2/Sparse   0    60    30.0.0.1    1

iss# show ip pim interface vlan 1

Address IfName/IfId Ver/Mode Nbr   Qry    DR-Address DR-Prio
                        Count Interval
10.0.0.1  vlan1/160 2/Sparse   0    45    10.0.0.1    5

iss# show ip pim interface detail

vlan1 33 is up
Internet Address is 12.0.0.1
Multicast Switching : Enabled
PIM : Enabled
PIMv6 : Disabled
  PIM version : 2, mode: Dense
  PIM DR : 12.0.0.1
  PIM DR Priority : 1
  PIM Neighbour Count : 0
  PIM Hello/Query Interval : 90
  PIM Message Interval : 60
  PIM Override Interval : 0
```

```

PIM Lan Delay : 0
PIM Lan-Prune-Delay : Disabled
PIM Graft Retry Interval : 3
PIM State Refresh : Uncapable
PIM Component Id : 1
PIM domain border : disabled
PIM State Refresh Processing : enabled
PIM Refresh Origination : Disabled

```



It shows the list of Interface addresses, the mode of the interface, Designated Router on that interface, Hello Interval, Join/Prune Interval of the interface.

Related Commands

- **set ip pim** – Enables or disables PIM
- **ip multicast** – Enables PIM globally.
- **ip pim query-interval** – Sets the frequency at which PIM hello messages are transmitted on this interface
- **ip pim message-interval** – Sets the frequency at which PIM Join/Prune messages are transmitted on this PIM interface
- **ip pim bsr-candidate - value** – Sets the preference value for the local interface as a candidate bootstrap router
- **ip pim dr-priority** – Sets the designated router priority value configured for the router interface
- **ip pim override-interval** – Sets the override interval configured for router interface
- **ip pim lan-delay** – Sets the LanDelay configured for the router interface
- **set ip pim lan-prune-delay** – Sets the LanPruneDelay bit configured for the router interface to advertise the lan delay
- **no ip pim interface** – Deletes an interface at PIM level
- **debug ip pim** – Enables PIM trace

51.32 show ip pim neighbor

This command displays the router's PIM neighbors' information.

```
show ip pim neighbor [{ Vlan <vlan-id> | <interface-type> <interface-id> }]
```

Syntax Description	Vlan	- VLAN ID
	interface-type	- Interface Type
	interface-id	- Interface Identifier

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip pim neighbor vlan 1

Neighbour Address	IfName/Idx	Uptime/Expiry	Ver	DRPri /Mode	CompId	Override Interval	LanDelay
12.0.0.2	vlan1/33	00:00:45/275	v2	1	1	0	0



It shows the Neighbor Address, the interface used to reach the PIM Neighbor, the Up time (the time since this neighbor became the neighbor of the local router), Expiry Time (the min. time remaining before this PIM neighbor will be aged out), LAN delay and Override interval.

- Related Commands**
- **ip pim query-interval** – Sets the frequency at which PIM hello messages are transmitted on this interface
 - **ip pim message-interval** – Sets the frequency at which PIM Join/Prune messages are transmitted on this PIM interface
 - **ip pim bsr-candidate - value** – Sets the preference value for the local interface as a candidate bootstrap router

51.33 show ip pim rp-candidate

This command displays the candidate RP information.

```
show ip pim rp-candidate [ComponentId <1-255>]
```

Syntax Description **ComponentId** - Component ID

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip pim rp-candidate 2

```

CompId  GroupAddress  Group Mask  RPAAddress/Priority
    2      224.1.0.0    255.255.0.0    20.0.0.1/192

```



It shows the Group addresses, the Group Mask and the RP address that indicates the IP address of the Rendezvous Point (RP) for the listed PIM Sparse group.

- Related Commands**
- **rp-candidate rp-address** – Enables the address of the interface, which will be advertised as a Candidate-RP
 - **rp-candidate holdtime** – Sets the holdtime of the component when it is a candidate RP in the local domain
 - **rp-static rp-address** – Sets the address of the interface, which will be advertised as a Static-RP

51.34 show ip pim rp-set

This command displays the RP-set information.

show ip pim rp-set [rp-address]

Syntax Description	rp-address	- Indicates the IP address of the Rendezvous Point (RP) for the listed PIM Sparse group.
---------------------------	-------------------	--

Mode	Privileged EXEC Mode
-------------	----------------------

Package	Enterprise and Metro
----------------	----------------------

Example	<pre>iss# show ip pim rp-set PIM Group-to-RP mappings ----- Group Address: 224.1.0.0 Group Mask: 255.255.0.0 RP: 20.0.0.1 Component-Id: 2 Hold Time: 120, Expiry Time: 00:01:43</pre>
----------------	---



It shows details of the Group Prefix, RP address, Hold time and Expiry Time.

Related Commands	<ul style="list-style-type: none">• rp-candidate rp-address – Enables the address of the interface, which will be advertised as a Candidate-RP• set ip pim static-rp – Enables or disables the Static RP configuration Status
-------------------------	--

51.35 show ip pim bsr

This command displays the BSR information.

show ip pim bsr [Component-Id (1-255)]

Syntax Description **Component-Id** - Component ID

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip pim bsr 1

```
PIMv2 Bootstrap Configuration For Component 1
-----
This system is the Bootstrap Router (BSR)
  BSR Address: 10.0.0.1
  BSR Priority: 6, Hash Mask Length: 30
```

Related Command

- **ip pim bsr-candidate - value** – Sets the preference value for the local interface as a candidate bootstrap router
- **ip pim bsr-candidate - VLAN** - Sets the local interface as a candidate bootstrap router.

51.36 show ip pim rp-static

This command displays the static RP information.

show ip pim rp-static [ComponentId <1-255>]

Syntax Description **ComponentId** - Component ID

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip pim rp-static 2

```

Static-RP Enabled
  CompId  GroupAddress  Group Mask      RPAddress
    2      225.1.0.0      255.255.0.0     20.0.0.1
  
```

Related Command **set ip pim static-rp** – Enables or disables the Static RP configuration Status

51.37 show ip pim component

This command displays the component information.

show ip pim component [ComponentId <1-255>]

Syntax Description **ComponentId** - Component ID

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip pim component 1

```
PIM Component Information
-----
Component-Id: 1
  PIM Mode: sparse,    PIM Version: 2
  Elected BSR: 10.0.0.1
  Candidate RP Holdtime: 0
```

Related Commands

- **ip pim component** – Configures the PIM component in the router
- **ip pim componentId** – Adds the interface to the component

51.38 show ip pim thresholds

This command displays threshold configured for SPT, RP thresholds, and rate limit values for both SM (Sparse mode).

show ip pim thresholds

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip pim thresholds

```
PIM SPT Threshold Information
  Group Threshold: 0
  Source Threshold: 0
  Switching Period: 0

PIM SPT-RP Threshold Information
  Register Threshold: 0
  RP Switching Period: 0
  Register Stop rate limit: 5
```

- Related Commands**
- **set ip pim threshold** – Specifies the SPT group or source threshold when exceeded, switching to shortest path tree is initiated
 - **set ip pim spt-switchperiod** – Specifies the period (in seconds) over which the data rate is to be monitored for switching to shortest path tree
 - **set ip pim rp-threshold** – Specifies the threshold at which the RP initiates switching to source specific shortest path tree
 - **set ip pim rp-switchperiod** – Specifies the period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree
 - **set ip pim regstop-ratelimit-period** – Specifies the period over which RP monitors number of register packets after sending the register stop message
 - **set ip pim pmbr** – Enables or disables the PMBR (PIM Multicast Border Router) Status
 - **ip pim dr-priority** – Sets the designated router priority value configured for the router interface

51.39 show ip pim mroute

This command displays the PIM multicast information.

```
show ip pim mroute [ {compid(1-255) | group-address | source-address }
summary]
```

Syntax Description	compid	- Component ID
	group-address	- Indicates the PIM multicast group address using the listed RP
	source-address	- The network address which identifies the sources for which this entry contains multicast routing information
	summary	- Summary of PIM mroute information

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip pim mroute

```
IP Multicast Routing Table
-----
```

```
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
IIF State P: Pruned F: Forwarding A: Graft Ack Pending
Timers: Uptime/Expires
Interface State: Interface, State/Mode
```

```
PIM Multicast Routing Table For Component 1
(12.0.0.10,227.1.1.1) ,00:00:03/05:43:11
  Incoming Interface : vlan1 ,RPF nbr : NULL ,Route Flags : ---
  IIF State : P ,SRM Generation : Enabled
  Source Active Timer Value 210
  Source Active Remaining Time : 05:43:11
  State Refresh Remaining Time : 00:00:00
  Prune Limit Remaining Time : 00:00:00
  Outgoing Interface List : NULL
```

```
iss# show ip pim mroute 1 summary
```

```
IP Multicast Routing Table
-----
```

```
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
Timers : Uptime/Expires
```

Interface State : Interface, State/Mode

```
PIM Multicast Routing Table For Component 1
(*, 224,1,0.0) , 00:04:35/--- , RP : 12.0.0.1
Incoming Interface : vlan1, RPF nbr : NULL, Route Flags : WR
Outgoing InterfaceList:
  vlan2, Forwarding/Sparse, 00:04:35/---

(12.0.0.30,224.1.0.0) , 00:00:04/00:03:26
Incoming Interface : vlan1, RPF nbr : NULL, Route Flages : S
Outgoing InterfaceList :
  vlan2, Forwarding/Sparse , 00:00:04/---
```



It shows details of the (S,G) ,(*,G) and (*,*,RP) entries.

**Related
Command**

ip pim bsr-candidate - value – Sets the preference value for the local interface as a candidate bootstrap router

51.40 show ip pim redundancy state

This command displays the status of PIM HA feature (enabled/disabled), status of active and standby PIM instance and status of dynamic bulk update.

show ip pim redundancy state

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip pim redundancy state

Hot-standby feature is Enabled.
Node State: Active, Standby Down .
Dynamic Bulk Updates not started

51.41 show ip pim redundancy shadow-table

This command displays the shadow-table information for PIMv4 Route entries.

show ip pim redundancy shadow-table

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip pim redundancy shadow-table

```
Forwarding Plane Shadow Table :
-----
(S, G)
Incoming interface:( Alias / IfIndex)
CPU Port Flag      :CPU Port Added / CPU Port Not Added
Route Mode         : Sparse / Dense
Route Status       : UnProcessed/Refreshed /New
Outgoing InterfaceList :( Alias / IfIndex)

(80.0.0.2, 224.6.6.6)
Incoming interface:(vlan4 / 38)
CPU Port Flag      :CPU Port Not Added
Route Mode         :Dense
Route Status       :New
Outgoing InterfaceList :
                    (vlan2 / 36), (vlan14 / 34),

(80.0.0.3, 224.6.6.6)
Incoming interface:(vlan4 / 38)
CPU Port Flag      :CPU Port Not Added
Route Mode         :Dense
Route Status       :New
Outgoing InterfaceList :
                    (vlan2 / 36), (vlan14 / 34),

Number of Entries : 2
```


Chapter

52

PIMv6

PIMv6 is a portable software implementation of the PIM (Sparse Mode and Dense Mode) specification, for IPv6 networks. The **Interface Masters PIMv6** provides support for inter-domain routing between domains using PIMv6-SM or PIMv6-DM. It also avoids the performance problems of earlier multicast routing protocols. This software provides multicast routing and forwarding capability to a router that runs the IPv6 protocol along with MLD (Multicast Listener Discovery). The **Interface Masters PIMv6** routes multicast data packets independent of any unicast routing protocol.

The list of CLI commands for the configuration of PIMv6 is as follows:

- set ipv6 pim
- set ip pim threshold
- set ip pim spt-switchperiod
- set ip pim rp-threshold
- set ip pim rp-switchperiod
- set ip pim regstop-ratelimit-period
- set ip pim pmbr
- set ip pim static-rp
- ip pim component
- ipv6 pim rp-candidate rp-address
- ipv6 pim rp-static rp-address
- ipv6 pim query-interval

- ipv6 pim message-interval
- ipv6 pim bsr-candidate
- ipv6 pim componentId
- ipv6 pim hello-holdtime
- ipv6 pim dr-priority
- ipv6 pim override-interval
- ipv6 pim lan-delay
- set ipv6 pim lan-prune-delay
- no ipv6 pim interface
- debug ipv6 pim
- show ipv6 pim interface
- show ipv6 pim neighbor
- show ipv6 pim rp-candidate
- show ipv6 pim rp-set
- show ipv6 pim bsr
- show ipv6 pim rp-static
- show ipv6 pim component
- show ipv6 pim thresholds
- show ipv6 pim mroute
- show ip pim redundancy state

52.1 show ip pim redundancy state

This command displays the status of PIM HA feature (enabled/disabled), status of active and standby PIM instance and status of dynamic bulk update.

show ip pim redundancy state

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip pim redundancy state

Hot-standby feature is Enabled.
Node State: Active,Standby Down .
Dynamic Bulk Updates not started

Related Commands

- show ipv6 pim redundancy shadow-table

52.2 set ipv6 pim

This command enables or disables PIMv6 globally.

```
set ipv6 pim { enable | disable }
```

Syntax Description	enable	- Enables PIMv6
	disable	- Disables PIMv6

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults disable

Example `iss (config)# set ipv6 pim enable`



When PIMv6 is globally enabled, the mode will be sparse.

Related Command `show ipv6 pim interface` – Displays the PIMv6 interfaces of the router

52.3 set ip pim threshold

This command configures the (Shortest Path Tree) SPT group or source threshold, when exceeded, switching to shortest path tree is initiated. To switch to SPT, the threshold MUST be configured.

```
set ip pim threshold { spt-grp | spt-src } < number of packets (0-2147483647) >
```

Syntax Description	spt-grp	- The threshold of data rate for any group. When exceeded, source specific counters are initiated for that particular group. It is based on number of bits per second
	spt-src	- The switching to Shortest Path Tree is initiated when the threshold of data rate for any source is exceeded. It is based on number of bits per second
	number of packets	- Number of packets
Mode	Global Configuration Mode	
Package	Enterprise and Metro	
Defaults	0	
Example	iss (config)# set ip pim threshold spt-grp 50	
Related Command	show ipv6 pim thresholds – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM	

52.4 set ip pim spt-switchperiod

This command configures the period (in seconds) over which the data rate is to be monitored for switching to shortest path tree.

```
set ip pim spt-switchperiod <0-2147483647(in secs)>
```

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults 0

Example `iss (config)# set ip pim spt-switchperiod 60`



- The same period is used for monitoring the data rate for both source and group. To switch to SPT, this period must be configured.
- The SPT is used for multicast transmission of packets with the shortest path from sender to recipients.

Related Command `show ipv6 pim thresholds` – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM

52.5 set ip pim rp-threshold

This command sets the threshold at which RP (Rendezvous Point) initiates switching to source specific shortest path tree.

set ip pim rp-threshold <0-2147483647(number of reg packets)>

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults 0

Example `iss (config)# set ip pim rp-threshold 50`



To switch to SPT, this threshold must be configured and this switching is based on the received number of registered packets.

Related Command **show ipv6 pim thresholds** – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM

52.6 set ip pim rp-switchperiod

This command sets the period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree.

```
set ip pim rp-switchperiod <0-2147483647(in secs)>
```

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults 0

Example `iss (config)# set ip pim rp-switchperiod 100`



- To switch to SPT, this period must be configured
- RP-tree is a pattern that multicast packets are sent to a PIM-SM router by unicast and then forwarded to actual recipients from RP

Related Command `show ipv6 pim thresholds` – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM

52.7 set ip pim regstop-ratelimit-period

This command sets the period over which RP monitors the number of register packets after sending the register stop message.

```
set ip pim regstop-ratelimit-period <0-2147483647(in secs)>
```

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults 5

Example `iss (config)# set ip pim regstop-ratelimit-period 100`



The Register Stop Message is used to avoid encapsulation of multicast data packets from the first hop router to the RP.

Related Command `show ipv6 pim thresholds` – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM

52.8 set ip pim pmbr

This command enables or disables the PMBR (PIM Multicast Border Router) Status.

```
set ip pim pmbr { enable | disable }
```

Syntax Description	enable	- Enables the PMBR Status
	disable	- Disables the PMBR Status

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults disable

Example `iss (config)# set ip pim pmbr enable`



- A PMBR integrates two different PIM domains (either PIM -SM or PIM -DM)
- A PMBR connects a PIM domain to other multicast routing domain(s)

Related Command `show ipv6 pim thresholds` – Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM

52.9 set ip pim static-rp

This command enables or disables the Static RP configuration Status. This command specifies whether to use the configured static- RP.

```
set ip pim static-rp { enable | disable }
```

Syntax Description	enable	- Enables the Static RP configuration Status
	disable	- Disables the Static RP configuration Status

Mode	Global Configuration Mode
-------------	---------------------------

Package	Enterprise and Metro
----------------	----------------------

Defaults	disable
-----------------	---------

Example	iss (config)# set ip pim static-rp enable
----------------	---

Related Commands	<ul style="list-style-type: none">• show ipv6 pim rp-set – Displays the RP-set information• show ipv6 pim rp-static – Displays the RP-static information
-------------------------	---

52.10 ip pim component

This command configures the PIMv6 component in the router and the no form of the command destroys the PIMv6 component.

```
ip pim component <ComponentId (1-255)>
```

```
no ip pim component <ComponentId (2-255)>
```

Mode Global Configuration Mode

Package Enterprise and Metro

Example iss (config)# ip pim component 1



- PIMv6 component 1 cannot be deleted as it is the default component.
- The PIMv6 Component corresponds to each instance of a PIMv6 domain and classifies it as Sparse or Dense mode.

Related Command `show ipv6 pim component-` Displays the component information

52.11 ipv6 pim rp-candidate rp-address

This command sets the address of the interface, which will be advertised as a Candidate-RP. The no form of the command disables the address of the interface, which will be advertised as a Candidate-RP.

```
ipv6 pim rp-candidate rp-address <Group Address> <Group Mask> <RP-address>
```

```
no ipv6 pim rp-candidate rp-address <Group Address> <Group Mask> <RP address>
```

Syntax Description	Group Address	- IPv6 multicast group address
	Group Mask	- IPv6 multicast group address mask that gives the group prefix for which the entry contains information about RP
	RP address	- IPv6 address of the Rendezvous Point

Mode PIM Component Mode

Package Enterprise and Metro

Example

```
iss(pim-comp)# ipv6 pim rp-candidate rp-address ff02::e001:0000
112 3333::1111
```



A Candidate-RP is a router configured to send periodic Candidate-RP-Advertisement messages to the BSR, and processes Join/Prune or Register messages for the advertised group prefix, when it is elected as a RP.

- Related Commands**
- **show ipv6 pim rp-set** – Displays the PIMv6 RP-set information
 - **show ipv6 pim rp-candidate** – Displays the PIMv6 RP-candidate information

52.12 ipv6 pim rp-static rp-address

This command sets the address of the IPv6 interface, which will be advertised as a Static-RP. The no form of the command disables the address of the IPv6 interface, which will be advertised as a Static-RP.

```
ipv6 pim rp-static rp-address <Group Address> <Group Mask> <RP address>
```

```
no ipv6 pim rp-static rp-address <Group Address> <Group Mask>
```

Syntax Description	Group Address	- Indicates the PIMv6 Sparse multicast group address using the listed RP
	Group Mask	- IPv6 multicast group address mask that gives the group prefix for which this entry contains information about RP
	RP address	- IPv6 address of the Rendezvous Point

Mode PIM Component Mode

Package Enterprise and Metro

Example

```
iss(pim-comp)# ipv6 pim rp-static rp-address ff02::e001:0000 112
3333::1111
```



The Static configuration allows additional structuring of the multicast traffic by directing the multicast join/prune messages to statically configured RPs.

Related Commands **show ipv6 pim rp-static** – Displays the RP-static information

52.13 ipv6 pim query-interval

This command sets the frequency at which PIMv6 hello messages are transmitted on the interface. The no form of the command sets the default hello timer interval for the interface.

```
ipv6 pim query-interval <Interval (0-65535) secs>
```

```
no ipv6 pim query-interval
```

Mode	Interface Configuration Mode
-------------	------------------------------

Package	Enterprise and Metro
----------------	----------------------

Defaults	30
-----------------	----

Example	iss (config-if)# ipv6 pim query-interval 60
----------------	---



The query message informs the presence of a PIMv6 router on the interface to the neighboring PIMv6 routers.

Related Command	show ipv6 pim interface – Displays the PIMv6 interfaces of the router
------------------------	--

52.14 ipv6 pim message-interval

This command sets the frequency at which the PIMv6 Join/Prune messages are transmitted on the PIMv6 interface. The no form of the command sets the default value for the PIMv6 Join/Prune messages.

```
ipv6 pim message-interval <Interval (0-65535)>
```

```
no ipv6 pim message-interval
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 60

Example iss (config-if)# ipv6 pim message-interval 120



The Join/Prune message interval used on all the PIMv6 routers in the PIMv6 domain must be the same. If all the routers do not use the same timer interval, the performance of PIMv6 Sparse can be adversely affected.

Related Command **show ipv6 pim interface** – Displays the PIMv6 interfaces of the router

52.15 **ipv6 pim bsr-candidate**

This command sets the preference value for the local PIMv6 interface as a candidate bootstrap router. The no form of the command sets the default preference value for the local PIMv6 interface as a candidate bootstrap router.

```
ipv6 pim bsr-candidate <value (0-255)>
```

```
no ipv6 pim bsr-candidate
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 0

Example iss (config-if)# `ipv6 pim bsr-candidate 1`



A BSR is a dynamically elected router within the PIMv6 domain.

Related Command `show ipv6 pim bsr` – Displays the PIMv6 BSR information

52.16 **ipv6 pim componentId**

This command adds the interface to the component.

ipv6 pim componentId <value(1-255)>

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 1

Example `iss (config-if)# ipv6 pim componentId 1`



This command adds the current VLAN into the specified PIMv6 component.

**Related
Commands**

- **set ipv6 pim** – Enables or disables PIMv6 globally
- **show ipv6 pim component** – Displays the component information

52.17 ipv6 pim hello-holdtime

This command sets the holdtime for the hello message for the PIMv6 interface. The no form of the command sets the default holdtime for the hello message for the interface.

```
ipv6 pim hello-holdtime <holdtime(1-65535)>
```

```
no ipv6 pim hello-holdtime
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 105

Example `iss (config-if)# ipv6 pim hello-holdtime 180`



Holdtime is the amount of time a receiver must keep the neighbor reachable, in seconds.

Related Commands

- `show ipv6 pim neighbor` – Displays the PIMv6 neighbor(s) information of the router

52.18 **ipv6 pim dr-priority**

This command sets the designated router priority value configured for the PIMv6 router interface. The no form of the command sets the default designated router priority value for the PIMv6 router interface.

```
ipv6 pim dr-priority <priority(1-65535)>
```

```
no ipv6 pim dr-priority
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 1

Example iss (config-if)# ipv6 pim dr-priority 100



The DR sets up multicast route entries and sends corresponding Join/Prune and Register messages on behalf of directly-connected receivers and sources, respectively.

Related Command **show ipv6 pim interface** – Displays the PIMv6 interfaces of the router

52.19 ipv6 pim override-interval

This command sets the override interval configured for the PIMv6 router interface. The no form of the command sets the default override interval for the PIMv6 router interface.

```
ipv6 pim override-interval <interval (0-65535)>
```

```
no ipv6 pim override-interval
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 0

Example `iss (config-if)# ipv6 pim override-interval 100`



The Override interval is the random amount of time delayed for sending override messages to avoid synchronization of override messages when multiple downstream routers share a multi-access link.

Related Command `show ipv6 pim interface` – Displays the PIMv6 interfaces of the router

52.20 ipv6 pim lan-delay

This command sets the LanDelay configured for the PIMv6 router interface. The no form of the command sets the default LanDelay for the PIMv6 router per interface.

```
ipv6 pim lan-delay <value(0-65535)>
```

```
no ipv6 pim lan-delay
```

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults 0

Example iss (config-if)# ipv6 pim lan-delay 120



The LAN Delay inserted by a router in the LAN Prune Delay option expresses the expected message propagation delay on the interface. It is used by upstream routers to find out the delayed time interval for a Join override message before pruning an interface.

Related Command **show ipv6 pim interface** – Displays the PIMv6 interfaces of the router

52.21 set ipv6 pim lan-prune-delay

This command sets the LanPruneDelay bit configured for the PIMv6 router interface to advertise the Lan delay. The command specifies whether to use LAN prune delay or not.

```
set ipv6 pim lan-prune-delay { enable | disable }
```

Syntax Description	enable	- Enables LAN-prune-delay
	disable	- Disables LAN-prune-delay

Mode Interface Configuration Mode

Package Enterprise and Metro

Defaults disable

Example iss (config-if)# set ipv6 pim lan-prune-delay enable

Related Command **show ipv6 pim interface** – Displays the PIMv6 interfaces of the router

52.22 **no ipv6 pim interface**

This command deletes the IPv6 PIM Interface, that is, this command is used to destroy the interface at PIMv6.

no ipv6 pim interface

Mode Interface Configuration Mode

Package Enterprise and Metro

Example `iss (config-if)# no ipv6 pim interface`

Related Command **show ipv6 pim interface** – Displays the PIMv6 interfaces of the router

52.23 debug ipv6 pim

This command enables PIMv6 trace and the no form of the command disables PIMv6 trace.

```
debug ipv6 pim {[nbr][grp][jp][ast][bsr][io][pmbr][mrt][mdh][mgmt][srm] [red]
| [all]}
```

```
no debug ipv6 pim {[nbr][grp][jp][ast][bsr][io][pmbr][mrt][mdh][mgmt][srm]
[red] | [all]}
```

Syntax Description	nbr	- Neighbor Discovery traces
	grp	- Group Membership traces
	jp	- Join or Prune traces
	ast	- Assert state traces
	bsr	- Bootstrap/RP traces
	io	- Input Output traces
	pmbr	- Interoperability traces
	mrt	- Multicast Route Table Update traces
	mdh	- Multicast Data Handling traces
	mgmt	- Configuration traces
	srm	- State Refresh Messages
	red	- Redundancy traces
	all	- All traces
Mode	Privileged EXEC Mode	

ISS

Package Enterprise and Metro

Example `iss # debug ipv6 pim all`



A Four byte integer value is specified for enabling the level of debugging. Each bit in the four byte integer variable represents a level of debugging. Combinations of levels are also allowed. The user has to enter the corresponding integer value for the bit set.

Related Command `show ipv6 pim interface`— Displays the PIMv6 interfaces of the router

52.24 show ipv6 pim interface

This command displays the PIMv6 interfaces of the router. It shows the list of Interface addresses, the mode of the interface, Designated Router on that interface, Hello Interval, Join/Prune Interval of the interface.

```
show ipv6 pim interface [{ Vlan <vlan-id> | detail }]
```

Syntax Description	Vlan	- VLAN ID
	detail	- Detailed information of the interface

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ipv6 pim interface

Address	IfName/ IfId	Ver/ Mode	Nbr Count	Qry Interval	DR Address	DR Prio-
fe80::2:a00:1	vlan1/33	2/Sparse	0	150	fe80::2:a00:1	1
fe80::2:1400:1	vlan2/34	2/Sparse	0	30	fe80::2:1400:1	1
fe80::2:1e00:1	vlan3/35	2/Sparse	0	30	fe80::2:1e00:1	1

```
iss# show ipv6 pim interface vlan 1
```

Address	IfName/ IfId	Ver/ Mode	Nbr Count	Qry Interval	DR Address	DR Prio-
fe80::2:a00:1	vlan1/33	2/Sparse	0	150	fe80::2:a00:1	1

```
iss# show ipv6 pim interface detail
```

```
vlan1 33 is up
  Internet Address is fe80::2:a00:1
  Multicast Switching : Enabled
  PIM : Enabled
  PIMv6 : Enabled
    PIM version : 2, mode: Sparse
    PIM DR : fe80::2:a00:1
    PIM DR Priority : 1
    PIM Neighbour Count : 0
    PIM Hello/Query Interval : 150
```

```
PIM Message Interval : 200
PIM Override Interval : 0
PIM Lan Delay : 0
PIM Lan-Prune-Delay : Disabled
PIM Component Id : 1
PIM domain border : disabled
```

**Related
Commands**

- **set ipv6 pim** – Enables or disables PIMv6
- **ipv6 pim query-interval** – Sets the frequency at which PIMv6 hello messages are transmitted on the interface
- **ipv6 pim message-interval** – Sets the frequency at which PIMv6 Join/Prune messages are transmitted on the PIMv6 interface
- **ipv6 pim bsr-candidate** – Sets the preference value for the local PIMv6 interface as a candidate bootstrap router
- **ipv6 pim dr-priority** – Sets the designated router priority value configured for the PIMv6 router interface
- **ipv6 pim override-interval** – Sets the override interval configured for the PIMv6 router interface
- **ipv6 pim lan-delay** – Sets the LanDelay configured for the PIMv6 router interface
- **set ipv6 pim lan-prune-delay** – Sets the LanPruneDelay bit configured for the PIMv6 router interface to advertise the lan delay
- **no ipv6 pim interface** – Deletes an interface at PIMv6 level
- **debug ipv6 pim** – Enables PIMv6 trace

52.25 show ipv6 pim neighbor

This command displays the PIMv6 neighbor(s) information of the router. It displays the Neighbor Address, the interface used to reach the PIMv6 Neighbor, the Up time (the time since this neighbor became the neighbor of the local router), Expiry Time (the minimum time remaining before this PIMv6 neighbor will be aged out), Lan delay and Override interval.

show ipv6 pim neighbor [Vlan <vlan-id>]

Syntax Description **Vlan** - VLAN ID

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ipv6 pim neighbor

Nbr Address	If Name /Idx	Uptime/ Expiry	Ver	DRPri/ Mode	Comp Id	Over- ride Interval	Lan Delay
fe80::2:a00:a	vlan1/33	00:02:33/0	v2	0/S	1	0	0
fe80::2:1400:a	vlan2/34	00:02:33/0	v2	0/S	1	0	0

iss# show ipv6 pim neighbor vlan 1

Nbr Address	If Name /Idx	Uptime/ Expiry	Ver	DRPri/ Mode	Comp Id	Over- ride Interval	Lan Delay
fe80::2:a00:a	vlan1/33	00:02:58/0	v2	0/S	1	0	0

Related Commands

- **ipv6 pim query-interval** – Sets the frequency at which PIMv6 hello messages are transmitted on the interface
- **ipv6 pim message-interval** – Sets the frequency at which PIMv6 Join/Prune messages are transmitted on the PIMv6 interface
- **ipv6 pim bsr-candidate** – Sets the preference value for the local PIMv6 interface as a candidate bootstrap router
- **ipv6 pim hello-holdtime** – Sets the holdtime for the hello message for the PIMv6 interface

52.26 show ipv6 pim rp-candidate

This command displays the PIMv6 RP-candidate information. It displays the Group addresses, the Group Mask and the RP address that indicates the IP address of the Rendezvous Point (RP) for the listed PIM Sparse group.

show ipv6 pim rp-candidate [ComponentId <1-255>]

Syntax Description **ComponentId** - Component ID

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ipv6 pim rp-candidate 1

CompId	GroupAddress/PrefixLength	RPAAddress/Priority
1	ff02::e000:0/112	3333::a00:1/192

- Related Commands**
- **ipv6 pim rp-candidate rp-address** – Sets the address of the interface, which will be advertised as a Candidate-RP
 - **ipv6 pim rp-static rp-address** – Sets the address of the interface, which will be advertised as a Static-RP

52.27 show ipv6 pim rp-set

This command displays the PIMv6 RP-set information. It displays details of the Group Prefix, RP address, Hold time and Expiry Time.

show ipv6 pim rp-set [rp-address]

Syntax Description	rp-address	- Indicates the IPv6 address of the Rendezvous Point (RP) for the listed PIM Sparse group.
---------------------------	-------------------	--

Mode	Privileged EXEC Mode
-------------	----------------------

Package	Enterprise and Metro
----------------	----------------------

Example	<pre>show ipv6 pim rp-set 3333::a00:a PIM Group-to-RP mappings ----- Group Address : ff00::Group Mask : 8 RP: 3333::a00:a Component-Id : 1 Hold Time : 102, Expiry Time : 00:00:35</pre>
----------------	---

Related Commands	<ul style="list-style-type: none">• ipv6 pim rp-candidate rp-address – Enables the address of the interface, which will be advertised as a Candidate-RP• ipv6 pim rp-static rp-address – Sets the address of the interface, which will be advertised as a Static-RP
-------------------------	--

52.28 show ipv6 pim bsr

This command displays the PIMv6 BSR information.

show ipv6 pim bsr [Component-Id (1-255)]

Syntax Description **Component-Id** - Component ID

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ipv6 pim bsr 1

```
PIMv2 Bootstrap Configuration For Component 1
-----
Elected BSR for Component 1
V6 BSR Address : 3333::a00:1
V6 BSR Priority : 100, Hash Mask Length : 126
This System is V6 Candidate BSR for Component 1
V6 BSR Address : 3333::a00:1
V6 BSR Priority : 100
```

Related Command **ipv6 pim bsr-candidate** – Sets the preference value for the local interface as a candidate bootstrap router

52.29 show ipv6 pim rp-static

This command displays the static RP information.

show ipv6 pim rp-static [ComponentId <1-255>]

Syntax Description **ComponentId** - Component ID

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ipv6 pim rp-static

Static-RP Enabled

CompId	GroupAddress/PrefixLength	RPAddress
1	ff02::1111:2222/64	3333::4444

Related Command **ipv6 pim rp-static rp-address** – Enables or disables the Static RP configuration Status

52.30 show ipv6 pim component

This command displays the component information.

```
show ipv6 pim component [ComponentId <1-255>]
```

Syntax Description	ComponentId - Component ID
---------------------------	-----------------------------------

Mode	Privileged EXEC Mode
-------------	----------------------

Package	Enterprise and Metro
----------------	----------------------

Example	<pre>iss# show ipv6 pim component 1 PIM Component Information ----- Component-Id: 1 PIM Mode: sparse, PIM Version: 2 Elected BSR: 10.0.0.1 Candidate RP Holdtime: 0</pre>
----------------	---

Related Commands	ipv6 pim componentId – Adds the interface to the component
-------------------------	---

52.31 show ipv6 pim thresholds

This command displays threshold configured for SPT, RP thresholds, and rate limit values for both SM and DM.

show ipv6 pim thresholds

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ipv6 pim thresholds

PIM SPT Threshold Information

```
-----  
Group Threshold   : 111  
Source Threshold  : 222  
Switching Period  : 100
```

PIM SPT-RP Threshold Information

```
-----  
Register Threshold      : 333  
RP Switching Period     : 300  
Register Stop rate limit : 400
```

**Related
Commands**

- **set ip pim threshold**— Configures the SPT group or source threshold
- **set ip pim spt-switchperiod**— Configures the period (in seconds) over which the data rate is to be monitored for switching to shortest path tree
- **set ip pim rp-threshold**— Sets the threshold at which the RP initiates switching to source specific shortest path tree
- **set ip pim rp-switchperiod**— Sets the period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree
- **set ip pim regstop-ratelimit-period**— Sets the period over which RP monitors number of register packets after sending the register stop message
- **set ip pim pmbr**— Enables or disables the PMBR (PIM Multicast Border Router) Status
- **ipv6 pim dr-priority**— Sets the designated router priority value configured for the router interface

52.32 show ipv6 pim mroute

This command displays the IPv6 PIM mroute information.

```
show ipv6 pim mroute [ {compid(1-255) | group <group-address> | source
<source-address> } summary ]
```

Syntax Description	compid	- Component ID
	group-address	- Indicates the PIMv6 multicast group address using the listed RP
	source-address	- The network address which identifies the sources for which this entry contains multicast routing information
	summary	- Summary of PIMv6 mroute information

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ipv6 pim mroute

```
IP Multicast Routing Table
-----
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
Timers: Uptime/Expires
Interface State: Interface, State/Mode

PIM Multicast Routing Table For Component 1
(*, ff02::e001:0) ,00:03:54/---3401:510a::3401:51a) Incoming
Interface : vlan1
,RPF nbr : fe80::2:a00:a ,Route Flags : WR
Outgoing InterfaceList :
    vlan2, Forwarding/Sparse ,00:03:54/---

iss# show ipv6 pim mroute group ff02::e001:0 summary

IP Multicast Routing Table
-----
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
Timers: Uptime/Expires

PIM Multicast Routing Table For Component 1
(*, ff02::e001:0) ,00:02:49/---3401:510a::3401:51a) ,Route Flags
```

: WR

```
iss# show ipv6 pim mroute source ca8d:5102::ca8d:5102 summary
```

IP Multicast Routing Table

Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit

Timers: Uptime/Expires

(ca8d:5102::ca8d:5102,ff02::e001:0) ,00:01:04/04:01:45 ,Route
Flags : ---



It shows details of the (S,G) ,(*,G) and (*,*,RP) entries.

**Related
Command**

ipv6 pim bsr-candidate – Sets the preference value for the local IPv6 interface as a candidate bootstrap router

52.33 show ip pim redundancy state

This command displays the status of PIM HA feature (enabled/disabled), status of active and standby PIM instance and status of dynamic bulk update.

show ip pim redundancy state

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip pim redundancy state

Hot-standby feature is Enabled.
Node State: Active, Standby Down .
Dynamic Bulk Updates not started

52.34 show ipv6 pim redundancy shadow-table

This command displays the shadow-table information for PIMv6 Route entries.

show ipv6 pim redundancy shadow-table

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ipv6 pim redundancy shadow-table

```
Forwarding Plane Shadow Table :
-----
(S, G)
Incoming interface:( Alias / IfIndex)
CPU Port Flag      :CPU Port Added / CPU Port Not Added
Route Mode         : Sparse / Dense
Route Status       : UnProcessed/Refreshed /New
Outgoing InterfaceList :( Alias / IfIndex)

(8080::5000:2, ff01::e006:606)
Incoming interface:(vlan4 / 36)
CPU Port Flag      :CPU Port Not Added
Route Mode         :Dense
Route Status       :New
Outgoing InterfaceList :
                    (vlan14 / 38), (vlan2 / 34),

(8080::5000:3, ff01::e006:606)
Incoming interface:(vlan4 / 36)
CPU Port Flag      :CPU Port Not Added
Route Mode         :Dense
Route Status       :New
Outgoing InterfaceList :
                    (vlan14 / 38), (vlan2 / 34),

Number of Entries : 2
```


Chapter

53

DVMRP

DVMRP (Distance Vector Multicast Routing Protocol) is an Internet Routing Protocol that provides efficient mechanism for connectionless message multicast to a group of hosts across an inter-network. Distance Vector Multicast Routing Protocol, an interior gateway protocol (IGP) suitable for use within an autonomous system but not between different autonomous systems.

DVMRP is based on RIP. DVMRP combines many of the features of RIP with the Truncated Reverse Path Broadcasting (TRPB) algorithm. To allow experiments to traverse networks that do not support multicasting a mechanism called tunneling was developed. DVMRP tunnels multicast transmission within unicast packets that are reassembled into multicast data when they arrive at their destination.

The key differences between DVMRP and RIP are RIP routes and forwards datagrams to a particular destination. The purpose of DVMRP is to keep track of the return paths to the source of the multicast datagrams.

The list of CLI commands for the configuration of DVMRP is as follows:

- set ip dvmrp
- ip dvmrp prune-life-time
- debug ip dvmrp
- show ip dvmrp

53.1 set ip dvmrp

This command enables / disables DVMRP in the switch or on a specific interface.

```
set ip dvmrp { enable | disable }
```

Syntax Description

- | | |
|----------------|--------------------------------|
| enable | - Enables DVMRP in the switch |
| disable | - Disables DVMRP in the switch |

Mode

Global Configuration Mode / Interface Configuration Mode

Package

Enterprise and Metro

Defaults

disable

Example

```
iss(config)# set ip dvmrp enable
iss(config-if)# set ip dvmrp enable
```



- IGMP proxy service must be disabled in the system before enabling the DVMRP globally.
- DVMRP must be globally enabled before enabling on the specific interface.
- If DVMRP is disabled on an interface, the DVMRP parameters return to their default values.

Related Commands

- **no ip igmp proxy-service** - Disables IGMP Proxy service in the system
- **show ip dvmrp** – Displays the DVMRP details

53.2 ip dvmrp prune-life-time

This command sets the prune life time value. The no form of the command sets the prune life time to the default value (50 seconds).

```
ip dvmrp prune-life-time <time(1-7200secs)>
```

```
no ip dvmrp prune-life-time
```

Mode Global Configuration Mode

Package Enterprise and Metro

Defaults time - 50 seconds

Example iss(config)# ip dvmrp prune-life-time 100



DVMRP must be enabled globally prior to the execution of this command.

Related Commands

- **set ip dvmrp** – Enables / disables DVMRP in the switch
- **show ip dvmrp** – Displays the DVMRP details

53.3 debug ip dvmrp

This command enables debugging support for DVMRP. The no form of the command disables debugging support for DVMRP.

```
debug ip dvmrp { [neighbor] [group] [join-prune] [i/o] [mrt] [mdh] [mgmt] | all }
```

```
no debug ip dvmrp { [neighbor] [group] [join-prune] [i/o] [mrt] [mdh] [mgmt] | all }
```

Syntax Description	neighbor	- Neighbor Discovery messages
	group	- Group Membership messages
	join-prune	- Join or Prune messages
	i/o	- Input/Output messages
	mrt	- Multicast Route table update messages
	mdh	- Multicast Data Handling messages
	mgmt	- Management Configuration messages
	all	- All traces

Mode Privileged EXEC Mode

Package Enterprise and Metro

Defaults Debugging is disabled.

Example iss# debug ip dvmrp all



DVMRP must be enabled in the device prior to the execution of this command.

Related Commands

- **set ip dvmrp** – Enables / disables DVMRP in the switch / a specific interface
- **show ip dvmrp** – Displays the DVMRP details

53.4 show ip dvmrp

This command displays the DVMRP details.

```
show ip dvmrp { routes [{ vlan <vlan-id(1-4094)> | <interface-type>
<interface-id> }] | mroutes | nexthop | neighbor | info | prune }
```

Syntax Description

- | | |
|-----------------------|------------------------------|
| routes | - Unicast Routes for VLAN ID |
| vlan | - VLAN Identifier |
| interface-type | - Interface Type |
| interface-id | - Interface Identifier |
| mroutes | - Multicast Routes |
| nexthop | - Nexthop Routes |
| neighbor | - DVMRP neighbors |
| info | - Information |
| prune | - Prune |

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip dvmrp routes

```
Dvmrp Routing Table
-----
2.0.0.0/8[2] uptime [0d 20:49:41.00], expires [0d 00:01:50.00]
Status: Active
via 10.0.0.2, vlan1

10.0.0.0/8[1] uptime [0d 22:20:00.00], expires [0d 00:02:00.00]
Status: Local/NeverExpire
via 10.0.0.1, vlan1

iss# show ip dvmrp mroutes
```

Dvmrp Forward Information

```

-----
(2.0.0.0, 227.1.1.1)
Reverse Path Forwarding Neighbor/Interface : 10.0.0.2/(vlan1)
Interface State of Upstream neighbor : PRUNED   Expiry Time :
6000

```

```

iss# show ip dvmrp nexthop

```

Dvmrp NextHop Information

```

-----
SrcAddress/Mask : 2.0.0.0/255.0.0.0
NextHopIndex : 160 (vlan1), IfType : Branch, DF: True
Dependent Nbrs :10.0.0.1

```

```

iss# show ip dvmrp neighbor

```

Neighbour Information

```

-----
Neighbor      Interface      Up           Exp          GenId      Adjacency
Address              Time          Time
-----
10.0.0.2      vlan1      [0d 22:31:48.00]  3400      133      ESTABLISHED

```

```

iss# show ip dvmrp info

```

```

DVMRP is enabled in the switch
Dvmrp Version:0x3 (major) 0xff (minor)
GenerationId: 0, Total Routes: 0, Reachable Routes: 0
Prune Life Time: 50

```

Interface Information

```

-----
IfaceName/Id      Address      Metric      AdminStatus
-----
vlan1/160          10.0.0.1      1      DVMRP_ENABLED

```

```

iss# show ip dvmrp prune

```

Prune List :

```

NbrAddress/PruneTime : 20.0.0.20/28
NbrAddress/PruneTime : 20.0.0.10/38

```

Related
Commands

- **set ip dvmrp** – Enables / disables DVMRP in the switch / a specific interface
- **ip dvmrp prune-life-time** – Sets the prune life time value
- **debug ip dvmrp** – Enables debugging support for DVMRP

Chapter

54

IPv4 Multicasting

IPv4 is an agreed-upon set of protocols, or rules, that allow computers to communicate with each other by specifying the format of packets and the addressing scheme.

IP multicasting is the sending of a single datagram to multiple hosts on a network or inter-network. Of the three delivery methods supported by IP, multicasting is the method that is most practical for one-to-many delivery. Unlike IP multicasting, IP unicasting sends a separate datagram to each recipient host. IP broadcasting sends a single datagram to all hosts on a single network segment (also known as subnet), even to those not interested in receiving it. Recent trends toward multimedia applications such as video conferencing necessitate the use of multicasting to efficiently send traffic to multiple hosts.

The list of CLI commands for the configuration of IPv4 multicasting¹ is as follows:

- `ip multicast routing / ip multicast-routing`
- `ip mcast ttl-threshold`
- `ip mcast rate-limit`
- `show ip mroute`

¹ The IPv4 multicasting commands can be executed only in the Linux simulation environment

54.1 ip multicast routing

This command enables the forwarding of IP multicast packets. The no form of the command disables the forwarding of IP multicast packets.

ip multicast routing

no ip multicast routing

Mode	Global Configuration Mode
Package	Enterprise and Metro
Defaults	IP multicast routing is enabled.
Example	<code>iss(config)# ip multicast routing</code>

54.2 ip multicast-routing

This command enables the forwarding of IP multicast packets. The no form of the command disables the forwarding of IP multicast packets.

This command is a standardized implementation of the existing command; `ip multicast routing`. It operates similar to the existing command.

`ip multicast-routing`

`no ip multicast-routing`

Mode	Global Configuration Mode
Package	Enterprise and Metro
Defaults	IP multicast routing is enabled.
Example	<code>iss(config)# ip multicast-routing</code>

54.3 ip mcast ttl-threshold

This command sets the TTL (time-to-live) threshold for multicast router interface. The no form of the command removes the TTL threshold for multicast router interface.

```
ip mcast ttl-threshold <ttl-threshold (0-255)>
```

```
no ip mcast ttl-threshold <ttl-threshold (0-255)>
```

Syntax Description	ttl-threshold - TTL threshold. This value ranges between 0 and 255.
---------------------------	--

Mode	Interface Configuration Mode
-------------	------------------------------

Package	Enterprise and Metro
----------------	----------------------

Defaults	<u>0</u>
-----------------	----------

Example	iss(config-if)# ip mcast ttl-threshold 45
----------------	---



Any IP multicast datagrams with a TTL value less than the threshold are not forwarded out the interface.

The default value of 0 means all the multicast packets are forwarded out the interface.

54.4 ip mcast rate-limit

This command sets the rate limit value (in kbps) for multicast router interface. The no form of the command disables rate-limiting on the multicast router interface.

```
ip mcast rate-limit <rate-limit (kbps)>
```

```
no ip mcast rate-limit
```

Syntax Description	rate-limit	- Rate limit value, in kilobits per second, of forwarded multicast traffic on the interface.
---------------------------	-------------------	--

Mode	Interface Configuration Mode
-------------	------------------------------

Package	Enterprise and Metro
----------------	----------------------

Defaults	<u>0</u>
-----------------	----------

Example	iss(config-if)# ip mcast rate-limit 10
----------------	--



A rate-limit of 0 indicates that no rate limiting is done.

54.5 show ip mroute

This command displays the multicast route information.

show ip mroute

Mode Privileged EXEC Mode

Package Enterprise and Metro

Example iss# show ip mroute

```
IPv4 Multicast Routing Status : Enabled

Multicast Routing Information
-----
(S,G), uptime/expires
Multicast routing protocol, Upstream neighbor
Incoming interface : interface
Outgoing interface list :
    interface, state, uptime/expires

(20.0.0.10, 224.1.0.0), 0d 00:00:13.83/ 0d 00:01:30.23
PIM-SM, 0.0.0.0
Incoming interface: vlan 2
Outgoing interface list:
    vlan 1, Forwarding, 0d 00:00:13.82/0d 00:01:30.22
```

Chapter

55

TAC

Transmission and Admission Control (TAC) is a utility module that is used by multicast protocols for filtering multicast packets and multicast VLAN classification. The profile table and filter table present in the TAC module are built through administrator configuration. All configured addresses are stored as address ranges. When a report is received on a particular interface, the corresponding profile mapped to this interface is obtained and filter rule table is scanned to determine if a match exists for the address present in the incoming report. If the address is present in the profile with permission as permit, the reports are processed else they are dropped.

The list of CLI commands for the configuration of TAC is as follows:


- ip mcast profile / ip igmp profile
- set ip mcast profiling
- permit
- deny
- range
- profile active
- show ip mcast profile
- debug tacm

55.1 ip mcast profile

This command creates or modifies a multicast profile and enters to profile configuration mode. The profile once created will have the permission details configured. The client's source address is maintained in the entry with the permission type as allow or deny. The reports from the client are processed by matching it with the profile id. The no form of this command deletes a multicast profile.

```
ip mcast profile <profile-id> [description (128)]
```

```
no ip mcast profile <profile-id>
```

Syntax	<profile-id>	- Configures the profile identifier for the multicast profile entry. This value ranges between 1 and 4294967295.
Description	description (128)	- Configures the description for the clients' details..
Mode	Global configuration mode	
Package	Workgroup, Enterprise and Metro	
Example	iss(config)# ip mcast profile 1 sample	
	This command can be executed only if the profile ID is not configured for multicast VLAN classification and the multicast profile index is not configured for a downstream interface.	

Related Commands

- **no ip igmp snooping multicast-vlan profile** – Removes the profile ID to VLAN mapping for multicast VLAN classification.
- **ip igmp snooping ratelimit** – Configures the rate limit for a downstream interface in units of the number of IGMP packets per second.
- **ip igmp snooping limit** – Configures the maximum limit type for an interface.
- **ip igmp snooping filter-profileId** – Configures the multicast profile index for a downstream interface.
- **no ip igmp snooping filter-profileId** – Resets the multicast profile index to default value.
- **permit** – Configures the action for the profile as permit.
- **deny** – Configures the action for the profile as deny.
- **range** – Creates or modifies a filter.
- **profile active** – Activates the profile entry.
- **show ip mcast profile** – Displays the filters configured in the profile and the profile statistics.

55.2 ip igmp profile

This command creates or modifies a multicast profile and enters the profile configuration mode. The `no` form of the command deletes a multicast profile.

This command is a standardized implementation of the existing command; `ip mcast profile`. It operates similar to the existing command.

```
ip igmp profile <profile-id>
```

```
no ip igmp profile <profile-id>
```

Syntax Description	profile-id	- Profile identifier for the multicast profile entry. This value ranges between 1 and 4294967295.
---------------------------	-------------------	---

Mode	Global configuration mode
-------------	---------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Example	<code>iss(config)# ip igmp profile 1</code>
----------------	---



This command can be executed only if the profile ID is not configured for multicast VLAN classification and the multicast profile index is not configured for a downstream interface.

Related Commands

- `no ip igmp snooping multicast-vlan profile` – Removes the profile ID to VLAN mapping for multicast VLAN classification.
- `ip igmp snooping ratelimit` – Configures the rate limit for a downstream interface in units of the number of IGMP packets per second.
- `ip igmp snooping limit` – Configures the maximum limit type for an interface.
- `permit` - Configures the action for the profile as permit.
- `deny` – Configures the action for the profile as deny.
- `range` – Creates or modifies a filter.
- `profile active` – Activates the profile entry.
- `show ip mcast profile` – Displays the filters configured in the profile and the profile statistics.

55.3 set ip mcast profiling

This command enables /disables IGMP profiling in the switch.

set ip mcast profiling {enable/disable}

Syntax Description	enable	- Configures the profiling to be enabled. When enabled the profile is allowed to be created.
	disable	- Configures the profiling to be disabled. New profiles are not allowed to be created.
Mode	Global configuration mode	
Package	Workgroup, Enterprise and Metro	
Defaults	Profiling is enabled.	
Example	iss(config)# set ip mcast profiling enable	

55.4 permit

This command configures the action for the channels associated with this profile as permit. When the profile action is permit, the matching rule is executed. The IGMPv3 reports with specific source list is modified with the sources that are permitted and the denied sources are removed from the list.

permit

Mode Profile configuration mode

Package Workgroup, Enterprise and Metro

Defaults Profile action is deny

Example `iss(config-profile)# permit`



This command can be executed only if the profile is de-activate.

Related Commands

- `ip igmp snooping multicast-vlan profile` – Configures profile ID to VLAN mapping for multicast VLAN classification.
- `ip mcast profile` – Creates or modifies a multicast profile.
- `no profile active` – De-activates the profile entry.
- `show ip mcast profile` – Displays the filters configured in the profile and the profile statistics.

55.5 deny

This command configures the action for the profile as deny. When the profile action is deny, the matching rule is not found in the table. The client report is not processed.

deny

Mode	Profile configuration mode
Package	Workgroup, Enterprise and Metro
Defaults	The profile action is deny
Example	<code>iss(config-profile)# deny</code>



This command can be executed only if the profile is de-activate.

Related Commands	<ul style="list-style-type: none">• <code>ip mcast profile</code> – Creates or modifies a multicast profile.• <code>no profile active</code> – De-activates the profile entry.• <code>show ip mcast profile</code> – Displays the filters configured in the profile and the profile statistics.
-------------------------	---

55.6 range

This command creates or modifies a filter. The filter entry is created based on the range of address provided by the administrator. If address is not configured, it is considered as a wild card (that is, the address is configured as 0.0.0.0).

The no form of this command deletes a filter.

```
range <group-start-addr> [<group-end-addr>] [source <source-start-addr>
[<source-end-addr>]] [filter-mode {include | exclude}]
```

```
no range <group-start-addr> [<group-end-addr>] [source <source-start-addr>
[<source-end-addr>]]
```

Syntax Description	<group-start-addr>	- Configures the multicast group address, which would be the start of multicast group address range.
	<group-end-addr>	- Configures the multicast group address, which would be the end of multicast group address range.
	<source-start-addr>	- Configures the multicast source address, which would be the start of multicast source address range.
	<source-end-addr>	- Configures the multicast source address, which would be the end of multicast source address range.
	filter-mode	- Configures the type of packets to be filtered. include – Applies filter for include IGMP/MLD reports. exclude – Applies filter for exclude IGMP/MLD reports.

Mode Profile configuration mode

Package Workgroup, Enterprise and Metro

Default Any

Example iss(config-profile)# range 225.0.0.1 227.0.0.1 source 34.0.0.1
38.0.0.1 filter-mode include



- This command can be executed only if the profile is de-activate.

Related Commands

- **ip mcast profile** – Creates or modifies a multicast profile.
- **no profile active** – De-activates the profile entry.
- **show ip mcast profile** – Displays the filters configured in the profile and the profile statistics.

55.7 profile active

This command activates the profile entry. When active, the profile is matched with the client report. The no form of this command de-activates the profile entry.

profile active

no profile active

Mode Profile configuration mode

Package Workgroup, Enterprise and Metro

Example `iss(config-profile)# profile active`

Related Commands

- **ip igmp snooping multicast-vlan profile** – configures profile ID to VLAN mapping for multicast VLAN classification.
- **ip igmp snooping ratelimit** – Configures the rate limit for a downstream interface in units of the number of IGMP packets per second.
- **ip igmp snooping limit** – Configures the maximum limit type for an interface.
- **ip igmp snooping filter-profileId** – Configures the multicast profile index for a downstream interface.
- **permit** – Configures the action for the profile as permit.
- **deny** – Configures the action for the profile as deny.
- **range** – Creates or modifies a filter.
- **ip mcast profile** – Creates or modifies a multicast profile.

55.8 show ip mcast profile

This command displays the filters configured in the profile and the profile statistics.

show ip mcast profile [<profile-id>] [statistics]

Syntax Description **<profile-id>** - Displays the profile identifier for the multicast profile entry.

statistics - Displays the statistics about the particular profile.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ip mcast profile

```
Profile 1 sample
  permit
  range 225.0.0.1 227.0.0.1 source 34.0.0.1 38.0.0.1 mode
include
  range 227.0.0.1 227.0.0.1
  range 228.0.0.1 230.0.0.1 mode exclude
```

```
Profile 2
  range 225.0.0.1 227.0.0.1 mode include
  range 227.0.0.1 227.0.0.1
  range 228.0.0.1 230.0.0.1 source 40.0.0.1 45.0.0.1 mode
exclude
```

```
iss# show ip mcast profile statistics
```

```
Profile 1 sample
  Port Reference count 1
  Vlan Reference count 1
```

```
Profile 2
  Port Reference count 0
  Vlan Reference count 0
```

- Related Commands**
- **ip mcast profile / ip igmp profile** – Creates or modifies a multicast profile.
 - **permit** – Configures the action for the profile as permit.
 - **deny** – Configures the action for the profile as deny.
 - **range** – Creates or modifies a filter.
 - **ip igmp snooping multicast-vlan profile** – Configures profile ID to VLAN mapping for multicast VLAN classification.
 - **ip igmp snooping filter-profileId** – Configures the multicast profile index for a downstream interface.

55.9 debug tacm

This command enables the generation of trace messages in TAC module. Trace messages are generated when there is an error, event or occurrence of a specified action in the module. The no form of this command disables the generation of trace messages.

```
debug tacm {all | [entry] [exit] [filter] [critical] [init-shut] [mgmt] [ctrl]
[resource] [all-fail]}
```

```
no debug tacm {all | [entry] [exit] [filter] [critical] [init-shut] [mgmt]
[ctrl] [resource] [all-fail]}
```

Syntax Description	all	- Generates trace messages for all types of traces
	entry	- Generates trace messages for all functions entered in the module.
	exit	- Generates trace messages for all the functions exited.
	filter	- Generates trace messages for filter related events.
	critical	- Generates traces messages for critical errors which need immediate attention.
	init-shut	- Generates trace messages for initialization and shutdown.
	mgmt	- Generates debug statements for management plane functionality traces.
	ctrl	- Generates debug statements for control plane functionality traces.
	resource	- Generates debug statements for traces with respect to allocation and freeing of all resource except the buffers.
	all-fail	- Generates trace messages for all types of failures.

Mode Privileged EXEC Mode

Example iss# debug tacm critical

Chapter

56

RMON

RMON (Remote Monitoring) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data.

The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

The list of CLI commands for the configuration of RMON is as follows:

- set rmon
- rmon collection history
- rmon collection stats
- rmon event
- rmon alarm
- show rmon

56.1 set rmon

This command is used to enable or disable the RMON feature.

```
set rmon {enable | disable}
```

Syntax Description	enable	- Enables the RMON feature in the system. On enabling, the RMON starts monitoring the networks both local and remote and provides network fault diagnosis
	disable	- Disables the RMON feature in the system. On disabling, the RMON's network monitoring is called off.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Disabled

Example `iss(config)# set rmon enable`

Related Command	• rmon collection history – Enables the history collection of interface statistics in the buckets for the specified time interval.
	• rmon collection stats - Enables RMON statistic collection on the interface
	• rmon event - Adds an event to the RMON event table
	• rmon alarm - Sets an alarm on a MIB object
	• show rmon - Displays the RMON statistics, alarms, events, and history configured on the interface

56.2 rmon collection history

This command enables history collection of interface statistics in the buckets for the specified time interval. The no form of the command disables the history collection on the interface.

```
rmon collection history <index (1-65535)> [buckets <bucket-number (1-65535)>]
[interval <seconds (1-3600)>] [owner <ownername (127)>]
```

```
no rmon collection history <index (1-65535)>
```

Syntax Description	<index (1-65535)>	- Identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular level for a MIB object in the device. The value ranges between 1 and 65535.
	buckets<bucket-number (1-65535)>	- Configures the maximum number of buckets desired for the RMON collection history group of statistics. The polling cycle is the bucket interval where the interface statistics details are stored. The value ranges between 1 and 65535 seconds.
	interval<seconds (1-3600)>	- Configures the time interval over which the data is sampled for each bucket to collect the statistics. The value ranges between 1 and 3600.
	owner<ownername (127)>	- Allows the user to enter the name of the owner of the RMON group of statistics

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults

bucket number	-	50
interval	-	1800 seconds
owner	-	monitor

Example `iss(config-if)# rmon collection history 1 buckets 2 interval 20`



This command is executed only if rmon is set as enabled
RMON collection stats must be configured before

Related Command

- **set rmon** - Enable or disable the RMON feature.
- **show rmon** - Displays the history collection for the configured bucket (show rmon history [history-index (1-65535)>])

56.3 rmon collection stats

This command enables RMON statistic collection on the interface. The no form of the command disables RMON statistic collection on the interface.

```
rmon collection stats <index (1-65535)> [owner <ownername (127)>]
```

```
no rmon collection stats <index (1-65535)>
```

Syntax Description	<p><index (1-65535)> - Identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular level for a MIB object in the device. The value ranges between 1 and 65535.</p> <p>owner <ownername (127)> - Allows the user to enter the name of the owner of the RMON group of statistics</p>
---------------------------	--

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults owner - monitor

Example `iss(config-if)# rmon collection stats 1`



The RMON feature must be enabled for the successful execution of this command.

Related Command

- **set rmon** - Enable or disable the RMON feature.
- **show rmon** - Displays the RMON collection statistics (show rmon statistics [<stats-index (1-65535)>])

56.4 rmon event

This command adds an event to the RMON event table. The added event is associated with an RMON event number. The no form of the command deletes an event from the RMON event table.

```
rmon event <number (1-65535)> [description <event-description (127)>] [log]
[owner <ownername (127)>] [trap <community (127)>]
```

```
no rmon event <number (1-65535)>
```

Syntax Description **<number (1-65535)>** - Sets the number of events to be added in the event table.

description<event-description (127)> - Provides a description for the event

log - Creates an entry in the log table for each event.

owner<ownername (127)> - Displays the entity that are configured this entry.

trap<community (127)> - Generates a trap, The SNMP community string is to be passed for the specified trap.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config)# rmon event 1 log owner Interface Masters trap
netman
```



This command is executed only if rmon is set as enabled

Related Commands

- **rmon alarm** - Sets an alarm on a MIB object
- **show rmon** - Displays the RMON events (show rmon events)
- **show snmp community** - Configures the SNMP community details
- **set rmon** - Enable or disable the RMON feature.

56.5 rmon alarm

This command sets an alarm on a MIB object. The Alarm group periodically takes statistical samples from variables in the probe and compares them to thresholds that have been configured. The no form of the command deletes the alarm configured on the MIB object.

```
rmon alarm <alarm-number> <mib-object-id (255)> <sample-interval-time (1-65535)> {absolute | delta} rising-threshold <value (0-2147483647)> [rising-event-number (1-65535)] falling-threshold <value (0-2147483647)> [falling-event-number (1-65535)] [owner <ownername (127)>]
```

```
no rmon alarm <number (1-65535)>
```

Syntax	<alarm-number>/	-	Displays the value of the statistic during the last sampling period. This value remains available until the current sampling period is completed.
Description	<number (1-65535)>		
			For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This value is compared with the rising and falling thresholds. The value ranges between 1 and 65535.
	<mib-object-id (255)>	-	Identifies the mib object.
	<sample-interval-time (1-65535)>	-	Identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular level for a MIB object in the device. This value ranges between 1 and 65535 seconds.
	absolute	-	Compares the value of the selected variable with the thresholds at the end of the sampling interval.
	delta		Subtracts the value of the selected variable at the last sample from the current value, and the difference is compared with the thresholds at the end of the sampling interval.
	rising-threshold <value (0-2147483647)>	-	Configures the rising threshold value. If the startup alarm is set as Rising alarm or RisingOrFalling alarm and if the configured threshold value is reached, then an alarm is raised. When the current sampled value is greater than or equal to the configured Rising threshold, and the value at the last sampling interval is less than this configured threshold, a single event will be generated. The value ranges between 0 and 2147483647.

- <rising-event-number (1-65535)>** - Raises the index of the event, when the Rising threshold is reached. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. This value ranges between 1 and 65535.
- falling-threshold <value (0-2147483647)>** - Configures the falling threshold value. If the startup alarm is set as Falling alarm or RisingOrFalling alarm and if the configured threshold value is reached, then an alarm is raised. When the current sampled value is lesser than or equal to the configured Falling threshold, and the value at the last sampling interval is greater than this threshold, a single event will be generated. This value ranges between 0 and 2147483647
- <falling-event-number (1-65535)>** - Raises the index of the event when the Falling threshold is reached. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. This value ranges between 1 and 65535.
- owner<ownername (127)>** - Sets the entity that are configured this entry.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults By default, the least event number in the event table is assigned for the rising and falling threshold as its event number.

Example

```
iss(config)# rmon alarm 4
1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 2 absolute rising-
threshold 2 2 falling-threshold 1 2 owner Interface Masters
```



- The RMON Feature must be enabled for the successful execution of this command
- RMON events must have been configured
- RMON collection stats must be configured
- In **Interface Masters ISS**, we cannot monitor all the mib objects through RMON. This will be applicable only to the Ethernet interfaces

- Related Commands**
- **rmon collection stats** - Enables RMON statistic collection on the interface
 - **rmon event** - Adds an event to the RMON event table
 - **show rmon** - Displays the RMON alarms (show rmon alarms)
 - **set rmon** - Enable or disable the RMON feature.

56.6 show rmon

This command displays the RMON statistics, alarms, events, and history configured on the interface.

```
show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events] [history
[history-index (1-65535)] [overview]]
```

Syntax Description	statistics	-	Displays a collection of statistics for a particular Ethernet Interface. The probe for each monitored interface on this device measures the statistics.
	alarms	-	Displays the value of the statistic during the last sampling period. This value remains available until the current sampling period is completed.
	events	-	Generates events whenever an associated condition takes place in the device. The Conditions may be alarms. Alarms are generated when a sampled statistical variable value exceeds the defined threshold value. Alarm module calls events module
	history	-	Displays the history of the configured RMON
	overview	-	Displays only the overview of rmon history entries

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example

```
iss# show rmon statistics 2

RMON is enabled
Collection 2 on Gi0/2 is active, and owned by fsoft,
Monitors ifEntry.1.2 which has
Received 1240 octets, 10 packets,
2 broadcast and 10 multicast packets,
0 undersized and 1 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
# of packets received of length (in octets):
64: 0, 65-127: 10, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0

iss# show rmon

RMON is enabled
```

```
iss# show rmon history
```

```
RMON is enabled
Entry 1 is active, and owned by fsoft
Monitors ifEntry.1.1 every 3000 second(s)
Requested # of time intervals, ie buckets, is 3,
Granted # of time intervals, ie buckets, is 3,
Sample 1 began measuring at 0
Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
# of dropped packet events is 0
Network utilization is estimated at 0
Sample 2 began measuring at 0
Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
# of dropped packet events is 0
Network utilization is estimated at 0
```

```
iss# show rmon events
```

```
RMON is enabled

Event 1 is active, owned by
Description is
Event firing causes nothing,
Time last sent is Aug 27 18:30:01 2009

Event 2 is active, owned by
Description is
Event firing causes nothing,
Time last sent is Aug 27 18:31:36 2009
```

```
iss# show rmon alarms
```

```
RMON is enabled
Alarm 4 is active, owned by Interface Masters
Monitors 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 every 2
second(s)
Taking absolute samples, last value was 3
Rising threshold is 2, assigned to event 2
Falling threshold is 1, assigned to event 2
On startup enable rising or falling alarm
```

```
iss# show rmon statistics 2 alarms events history 1
```

```
RMON is enabled
Collection 2 on Ex0/1 is active, and owned by monitor,
Monitors ifEntry.1.1 which has
Received 5194 octets, 53 packets,
```

```

0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
53 CRC alignment errors and 0 collisions.
# of packets received of length (in octets):
64: 0, 65-127: 53, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0
Alarm 4 is active, owned by Interface Masters
Monitors 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 every 2
second(s)
Taking absolute samples, last value was 3
Rising threshold is 2, assigned to event 2
Falling threshold is 1, assigned to event 2
On startup enable rising or falling alarm

Event 1 is active, owned by
Description is
Event firing causes nothing,
Time last sent is Aug 27 18:30:01 2009

Event 2 is active, owned by
Description is
Event firing causes nothing,
Time last sent is Aug 27 18:31:36 2009

iss# show rmon history overview

RMON is enabled
Entry 1 is active, and owned by fsoft
Monitors ifEntry.1.1 every 3000 second(s)
Requested # of time intervals, ie buckets, is 3,
Granted # of time intervals, ie buckets, is 3

```



This command is executed only if rmon is set as enabled

Related Commands

- **set rmon** - Enables or disables the RMON feature
- **rmon collection history** - Enables history collection of interface statistics in the buckets for the specified time interval
- **rmon collection stats** - Enables RMON statistic collection on the interface
- **rmon event** - Adds an event to the RMON event table
- **rmon alarm** - Sets an alarm on a MIB object

Chapter

57

RMON2

RMONv2 is an extension of the RMON that deals with the information at the physical and data link network levels to support monitoring and protocol analysis of LANs. RMONv2 adds support for network and application layer monitoring.

RMONv2 is a portable implementation of Remote Network Monitoring version 2. RMONv2 is implemented with nine RMON Mib groups. They are Protocol directory, Protocol distribution, Address Map, Network Layer Host, Network Layer Matrix, Application Layer Host, Application layer Matrix, User History collection and Probe configuration groups. RMONv2 provides extensions to four RMONv1 tables. They are: etherStats table, historyControl table, hostControl table and matrixControl table. RMON should be enabled for configuring the RMONv1 tables

The list of CLI commands for the configuration of RMON2 is as follows:

- rmon2
- debug rmon2

57.1 rmon2

This command enables / disables RMON2 module in the switch. RMON2 lists the inventory of protocols, lists MAC address to network address bindings, tracks the amount of traffic between network addresses and so on. The default value is disabled.

rmon2 {enable | disable}

Syntax Description	enable	- Enables the RMON2 module in the switch. Resources are allocated to the module.
---------------------------	---------------	--

	disable	- Disables the RMON2 module in the switch. Resources allocated are released back to the system.
--	----------------	---

Mode	Global Configuration Mode
-------------	---------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	disabled
-----------------	----------

Example	<code>iss(config)# rmon2 enable</code>
----------------	--

57.2 debug rmon2

This command configures various RMON2 debug trace messages.. The no form of the command disables the debug feature for RMON2 module. Debug facility captures events,errors and the level of severity of the traces and logs them in a file.

```
debug rmon2 {[func-entry][func-exit][critical][mem-fail][debug] | [ALL]}
```

```
no debug rmon2
```

Syntax Description	func-entry	- Generates Function Entry Trace messages. When a function is called in the RMON2 module, the details of the function are displayed in the trace message. The traces are captured for all the functions in RMON2.
	func-exit	- Generates Function Exit Trace messages. When the system completes a function and exits, the details of the function exited is displayed in the trace messages. The traces are captured for all functions.
	critical	- Generates Critical Trace messages. The errors that cause damage or malfunctioning of the system are displayed as critical traces.
	mem-fail	- Generates Memory failure Trace messages. When there is a constraint for memory allocation when a fuction is initiated, the mem-fail trace is displayed.
	debug	- Generates Debug Trace messages for less severe errors and events.
	ALL	- Generates all kinds of trace messages mentioned above.
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	
Example	iss# debug rmon2 ALL	

Chapter

58

DSMON

DSMON (Differentiated Services Monitoring) is designed to monitor the network traffic usage of DSCP (Differentiated Services Code Point) values. It is a distributed network monitoring framework consisting of Probes, also called as Monitors/Agents. These are distributed throughout the network fabric and are controlled by a central manager. Central manager and the probes communicate each other using SNMP/CLI/WebNm. The Probes are capable of reading and writing to the local DSMON Mib in response to the Management action and performing various DSMON functions. The Monitor can provide summary information including error statistics such as count of undersized packets and number of collisions and performance statistics such as number of packets delivered per second and packet size distribution.

The list of CLI commands for the configuration of DSMON is as follows:

- dsmon
- debug dsmon

58.1 dsmon

This command configures DSMON module in the switch. The DSMON in enabled state configures counter aggregation profiles, provides statistics per data source per counter aggregation group, supports hardware forwarding and simulated hardware forwarding and so on.

dsmon {enable | disable}

Syntax Description	enable	- Enables the DSMON module in the switch. Monitor provides error statistics such as count of undersized packets and number of collisions and performance statistics such as number of packets delivered per second and packet size distribution.
	disable	- Disables the DSMON module in the switch. All the resources allocated is released back to the system.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults disabled

Example `iss(config)# dsmon enable`



RMON2 should be enabled before enabling DSMON.

Related Commands `rmon2` - Enables or disables the RMON2 software

58.2 debug dsmon

This command configures the DSMON debug trace messages. The no form of this command disables the debug trace message configurations for DSMON module. Debug facility captures events, errors and the level of severity of the traces and logs them in a file.

```
debug dsmon {[func-entry][func-exit][critical][mem-fail][debug] | [ALL]}
```

```
no debug dsmon
```

Syntax Description	func-entry	- Generates Function Entry Trace messages. When a function is called in the DSMON module, the details of the function are displayed in the trace message. The traces are captured for all the functions in DSMON.
	func-exit	- Generates Function Exit Trace messages. When the system completes a function and exits, the details of the function exited is displayed in the trace messages. The traces are captured for all functions.
	critical	- Generates Critical Trace messages. The errors that cause damage or malfunctioning of the system are displayed as critical traces.
	mem-fail	- Generates Memory failure Trace messages. When there is a constraint for memory allocation during the function initiation, the mem-fail trace is displayed
	debug	- Generates Debug Trace messages for less severe errors and events.
	ALL	- Generates all kinds of trace messages mentioned above.
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	
Example	iss# debug dsmon ALL	

Chapter

59

EOAM

The Ethernet Operations, Administration and Maintenance (EOAM) sub-layer provides mechanisms useful for monitoring link operation such as link monitoring, remote fault indication and remote loopback control. In general, OAM provides network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions. The EOAM optional sub-layer provides data link layer mechanisms that complement the application that may reside in higher layers.

The EOAM information is conveyed in Slow Protocol frames called OAM Protocol Data Units (OAMPDUs). The OAMPDUs contain the appropriate control and status information used to monitor, test and troubleshoot EOAM-enabled links. The OAMPDUs (untagged frames) traverse a single link, being passed between peer OAM entities, and as such, are not forwarded by MAC clients (bridges or switches).

The list of CLI commands for the configuration of EOAM is as follows:

- shutdown ethernet-oam
- set ethernet-oam
- ethernet-oam
- set ethernet-oam oui
- ethernet-oam link-monitor event-resend
- ethernet-oam link monitor set
- debug ethernet-oam
- ethernet-oam mode
- ethernet-oam remote-loopback – deny/permit
- ethernet-oam remote-loopback – enable/disable
- ethernet-oam link-monitor – link events

- ethernet-oam link-monitor – window size
- ethernet-oam link-monitor frame window
- ethernet-oam link-monitor frame-sec-summary window
- ethernet-oam link-monitor – threshold error count
- ethernet-oam link-monitor frame-sec-summary threshold
- ethernet-oam - critical-event / dying-gasp
- clear port ethernet-oam - statistics
- clear port ethernet-oam – event log
- show ethernet-oam global information
- show port ethernet-oam
- show port ethernet-oam - neighbor
- show port ethernet-oam - loopback-capabilities
- show port ethernet-oam - statistics
- show port ethernet-oam - event-log

59.1 shutdown ethernet-oam

This command shutdown EOAM in all the ports of the the system and releases the allocated resources. The no form of this command starts EOAM in the system and allocates the resources required by EOAM module.

shutdown ethernet-oam

no shutdown ethernet-oam

Mode Global Configuration Mode

Package Workgroup

Defaults Enabled

Example `iss(config)# shutdown ethernet-oam`



When shutdown, all resources acquired by the EOAM Module are released to the system.

**Related
Command**

- **set ethernet-oam** - Enables the EOAM in all ports of the system,
- **ethernet-oam** - Enables the EOAM in the port.
- **set ethernet-oam oui** - Configures the “Organization Unique Identifier” (OUI) of the local EOAM client.
- **ethernet-oam link-monitor event-resend** - Sets the resend count of OAMPDUs to be sent for event notification.
- **ethernet-oam link monitor set** - Sets the EOAM link monitoring functionality in the system.
- **ethernet-oam mode** - Configures the EOAM mode as either active or passive.
- **ethernet-oam remote-loopback - deny/permit** - Ignores or processes the remote EOAM loopback commands.
- **ethernet-oam remote-loopback - enable/disable** - Starts or stops EOAM Remote loopback.
- **ethernet-oam link-monitor - link events** - Enables or disables EOAM link event(s) monitoring functionality.
- **ethernet-oam link-monitor - window size** - Specifies the window size for link events for ethernet OAM link monitoring.
- **ethernet-oam link-monitor frame window** - Specifies the window size for the frame which is the amount of time over which the threshold is defined.
- **ethernet-oam link-monitor frame-sec-summary window** - Sets the window size for frame second summary
- **ethernet-oam link-monitor - threshold error count** - Sets the threshold error count for link monitoring
- **ethernet-oam link-monitor frame-sec-summary threshold** - Sets the threshold error count for frame seconds summary
- **ethernet-oam - critical-event / dying-gasp** - Enables/disables critical event or dying gasp fault indication
- **debug ethernet-oam** - Enables the debug level for the EOAM Module
- **clear port ethernet-oam - statistics** - Clears ethernet OAM configuration or statistics for all ports/specific port
- **clear port ethernet-oam - event log** - Clears the EOAM event log.
- **show ethernet-oam global information** - Displays the EOAM global configuration information
- **show port ethernet-oam - neighbor** - Displays EOAM local information of the neighbour
- **show port ethernet-oam - loopback-capabilities** - Displays the EOAM information of the loopback capabilities
- **show port ethernet-oam - statistics** - Displays the EOAM statistics related information
- **show port ethernet-oam - event-log** - Displays the EOAM event log.

59.2 set ethernet-oam

This command enables or disables EOAM in all the ports of the system. EOAM is used when ethernet is deployed as the broadband access technology between carrier and customer networks.

```
set ethernet-oam {enable | disable}
```

Syntax Description	enable	-	Enables the EOAM in the switch on all ports. It allows the user to monitor and troubleshoot Ethernet point-to-point links. EOAM must be enabled globally prior to enable it in individual ports.
---------------------------	---------------	---	--

	disable	-	Disables the EOAM in the switch on all ports.
--	----------------	---	---

Mode	Global Configuration Mode
-------------	---------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	Disable
-----------------	---------

Example	<code>iss(config)# set ethernet-oam enable</code>
----------------	---



This command executes only if ethernet oam is not set as shutdown.

Related Command	<ul style="list-style-type: none">• shutdown ethernet-oam - Shutdown EOAM in all the ports of the the system and releases the allocated resources.• show ethernet-oam global information - Displays EOAM global status
------------------------	---

59.3 ethernet-oam

This command enables or disables EOAM on a particular port.

ethernet-oam {disable | enable}

Syntax Description	disable	-	Disables EOAM on a port
	enable	-	Enables EOAM on a port which allows the user to monitor and troubleshoot Ethernet point-to-point links.

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults disable

Example

```
iss(config)# interface gigabitethernet 0/1
iss(config-if)# ethernet-oam enable
```



This command executes only if ethernet oam is not set as shutdown.

Related Command **show port ethernet-oam** - Displays EOAM local information

59.4 set ethernet-oam oui

This command configures the “Organization Unique Identifier” (OUI) of the local EOAM client. This value is sent in the information OAMPDU in local information TLV. The OUI is a 24-bit identifier that is purchased from IEEE to uniquely identify a vendor, manufacturer, or assignee. The no form of this command resets OUI to its default value.

```
set ethernet-oam oui <aa:aa:aa>
```

```
no ethernet-oam oui
```

Mode Global Configuration Mode

Package Workgroup

Defaults Default value corresponds to the first three bytes of the System MAC Address

Example `iss(config)# set ethernet-oam oui 02:03:04`



This command executes only if ethernet oam is not set as shutdown.

Related Command

- **shutdown ethernet-oam** - Shutdown EOAM in all the ports of the the system and releases the allocated resources.
- **show ethernet-oam global information** - Displays EOAM global status

59.5 ethernet-oam link-monitor event-resend

This command sets the resend count of OAMPDUs to be sent for Event Notification. The no form of the command resets the event resend count of OAMPDUs to its default value.

```
ethernet-oam link-monitor event-resend <count (1-10)>
```

```
no ethernet-oam link-monitor event-resend
```

Syntax description	<count (1 - 10)>	Configures the resend count which is the number of times an error event OAMPDU can be sent repeatedly. The events such as symbol period, frame-period, frame, frame-secs-summary and organization specific event are sent repeatedly, to avoid loss of OAMPDUs on faulty links. The count value ranges between 1 and 10.
---------------------------	------------------	--

Mode	Global Configuration Mode
-------------	---------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	10
-----------------	----

Example	iss(config)# ethernet-oam link-monitor event-resend 2
----------------	---



This command executes only if ethernet oam is not set as shutdown.

Related Command	<ul style="list-style-type: none"> • show ethernet-oam global information - Displays EOAM global status • shutdown ethernet-oam - Shutdown EOAM in all the ports of the the system and releases the allocated resources.
------------------------	--

59.6 ethernet-oam link monitor set

This command sets the EOAM link monitoring functionality in the system.

```
ethernet-oam link-monitor set { enable |disable }
```

Syntax Description	enable	-	Enables EOAM Link-Monitoring in the system
---------------------------	---------------	---	--

	disable	-	Disables EOAM Link-Monitoring in the system
--	----------------	---	---

Mode	Global Configuration Mode
-------------	---------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	Enable
-----------------	--------

Example	iss(config)# ethernet-oam link-monitor set disable
----------------	--



This command executes only if ethernet oam is not set as shutdown.

Related Commands	<ul style="list-style-type: none">• shutdown ethernet-oam - Shutdowns EOAM in all the ports of the the system and releases the allocated resources.
-------------------------	--


59.7 debug ethernet-oam

This command enables the debug level for the EOAM Module. When no arguments are given, this command displays the current debug level. The no form of the command disables debug option for the EOAM Module. It is also used to display the configured EOAM debug level.

```
debug ethernet-oam [all] [critical] [init] [resource] [failure] [pkt] [buffer]
[config] [discovery] [loopback] [lm] [var-reqresp] [rfi] [ctrl] [func-entry]
[func-exit] [mux-parser] [redundancy]
```

```
no debug ethernet-oam {[all] | [critical] [init] [resource] [failure] [pkt]
[buffer] [config] [discovery] [loopback] [lm] [var-reqresp] [rfi] [ctrl]
[func-entry] [func-exit] [mux-parser] [redundancy]}
```

Syntax	all	- Generates debug statements for all the traces.
Description		
	critical	- Generates debug statements for all Critical occasions
	init	- Generates debug statements for init traces. This trace is generated on failed initialization and shutting down of EOAM related entries
	resource	- Generates debug statements for OS resource related traces except buffer.
	failure	- Generates debug statements for all failure traces.
	pkt	- Generates debug statements for packet dump traces.
	buffer	- Generates debug statements for EOAM buffer related traces
	config	- Generates debug statements for EOAM configuration traces
	discovery	- Generates debug statements for EOAM discovery traces
	loopback	- Generates debug statements for EOAM remote loopback Traces
	lm	- Generates debug statements for EOAM link monitoring traces
	var-reqresp	- Generates debug statements for EOAM MIB Variable Request/Response traces
	rfi	- Generates debug statements for EOAM remote failure indication traces

	ctrl	-	Generates debug statements for control plane traces
	func-entry	-	Generates debug statements for function entry traces
	func-exit	-	Generates debug statements for function exit traces
	mux-parser	-	Generates debug statements for EOAM MUX parser traces
	redundancy	-	Generates debug statements for EOAM redundancy traces.
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	critical		
Example	<pre>iss# debug ethernet-oam all</pre>		
	 This command executes only if ethernet oam is not set as shutdown.		
Related Commands	<ul style="list-style-type: none">• show debugging- Displays state of each debugging option.• shutdown ethernet-oam - Shutdown EOAM in all the ports of the the system and releases the allocated resources.		

59.8 ethernet-oam mode

This command configures the EOAM mode as either active or passive.

ethernet-oam mode {active | passive}

Syntax Description	active	-	Sets the remote OAM entity in a loopback state and initiates monitoring activities with the remote OAM peer entity. The remote OAM entity echoes back every received frame (except OAMPDUs) over the same interface on which the frame is received. The normal traffic is disabled and the looped back frames are transmitted on the interface.
	passive	-	Does not set the remote OAM entity in the loopback state and waits for the peer to initiate OAM actions.
Mode	Interface Configuration Mode		

Package Workgroup, Enterprise and Metro

Defaults active

Example `iss(config-if)# ethernet-oam mode passive`



This command executes only if ethernet oam is not set as shutdown.

Related Command

- **show port ethernet-oam** - Displays EOAM local information
- **shutdown ethernet-oam** - Shutdown EOAM in all the ports of the the system and releases the allocated resources.

59.9 ethernet-oam remote-loopback – deny/permit

This command ignores or processes the remote EOAM loopback commands.

ethernet-oam remote-loopback {deny | permit}

Syntax Description	deny	-	Ignores the received loopback commands that are used to monitor the health of the link
---------------------------	-------------	---	--

	permit	-	Processes the OAM loopback commands that are used to monitor the health of the link
--	---------------	---	---

Mode	Interface Configuration Mode
-------------	------------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Defaults	deny
-----------------	------

Example	<code>iss(config-if)# ethernet-oam remote-loopback deny</code>
----------------	--



This command executes only if ethernet oam is not set as shutdown.

Related commands	<ul style="list-style-type: none">• ethernet-oam remote-loopback - enable/disable - Starts or stops the EOAM Remote loopback• show port ethernet-oam - Displays EOAM local information• show port ethernet-oam - loopback-capabilities - Displays EOAM loopback capabilities• shutdown ethernet-oam - Shutdown EOAM in all the ports of the the system and releases the allocated resources.
-------------------------	---

59.10 ethernet-oam remote-loopback – enable/disable

This command starts or stops EOAM Remote loopback.

The **ethernet-oam remote-loopback** must be set to 'permit' for starting the EOAM Remote loopback functionality between the OAM peers.

ethernet-oam remote-loopback {disable | enable}

Syntax Description	disable	- Stops EOAM Remote loopback
	enable	- Starts EOAM Remote loopback

Mode Interface Configuration Mode(Physical)

Package Workgroup, Enterprise and Metro

Example `iss(config-if)# ethernet-oam remote-loopback disable`



This command executes only if ethernet oam is not set as shutdown.

Related Commands

- **ethernet-oam remote-loopback - deny/permit** - Ignores or processes the EOAM loopback command
- **shutdown ethernet-oam** - Shutdown EOAM in all the ports of the the system and releases the allocated resources.

59.11 ethernet-oam link-monitor – link events

This command enables or disables EOAM link event(s) monitoring functionality.

```
ethernet-oam link-monitor [{symbol-period | frame | frame-period | frame-sec-
summary}] {enable | disable}
```

Syntax Description	symbol-period	- Sends an event notification OAMPDU when an errored symbol period event occurs and the EOAM link event(s) supports the monitoring functionality in the switch.
	frame	- Sends an event notification OAMPDU when an errored frame event occurs.
	frame-period	- Sends an event notification OAMPDU when an errored frame period event occurs
	frame-sec-summary	- Sends an event notification OAMPDU when an errored frame period summary event occurs
	enable	- Sends an event notification OAMPDU when an errored event occurs
	disable	- Does not send any event notification OAMPDU when an errored event occurs
Mode	Interface Configuration Mode(Physical)	
Package	Workgroup, Enterprise and Metro	
Defaults	enable	
Example	iss(config-if)# ethernet-oam link-monitor symbol-period enable	



- If the EOAM link-monitor is set to enable/disable without specifying any of the optional notification parameters, then event monitoring is enabled/disabled for all notifications.
- This command executes only if ethernet oam is not set as shutdown.

Related Commands	• show port ethernet-oam - Displays EOAM local information
	• shutdown ethernet-oam - Shutdowns EOAM in all the ports of the the system and releases the allocated resources.

59.12 ethernet-oam link-monitor – window size

This command specifies the window size for link events for ethernet OAM link monitoring. Symbol period and frame-period window size should be greater than threshold count. Symbol period window size is configured in units of millions. The no form of this command sets the window size to its default value.



The no form of this command is a subset of the combined form of the command for configuring the window and threshold parameters for the various types of link events.

```
ethernet-oam link-monitor {symbol-period | frame-period} window
<size(0xffff../123456..) >
```

```
no ethernet-oam link-monitor {symbol-period | frame | frame-period | frame-
sec-summary} {threshold | window}
```

Syntax Description	symbol-period	- Sends an event notification OAMPDU when an errored symbol period event occurs and the EOAM link event(s) supports the monitoring functionality in the switch.
	frame-period	- Sends an event notification OAMPDU when an errored frame period event occurs
	window <size(0xffff../123456..) >	Enters the number of symbols (millions) over which the Threshold event is defined.
	frame	Sends an event notification OAMPDU when an errored frame event occurs.
	frame-sec-summary	Sends an event notification OAMPDU when an errored frame period summary event occurs
	threshold	Sets the the number of symbol errors that must occur within a given Window for generating an Event notification OAMPDU.
	window	Sets the number of symbols (millions) over which the threshold event is defined.
Mode	Interface Configuration Mode(Physical)	
Package	Workgroup, Enterprise and Metro	
Defaults	symbol-period	625 millions
	frame	10
	frame-period	10 millions

Example `iss(config-if)# ethernet-oam link-monitor symbol-period window 20`



This command executes only if ethernet oam is not set as shutdown.

**Related
Commands**

- **show port ethernet-oam** - Displays EOAM local information
- **shutdown ethernet-oam** - Shutdown EOAM in all the ports of the the system and releases the allocated resources.

59.13 ethernet-oam link-monitor frame window

This command specifies the window size for the frame which is the amount of time over which the threshold is defined. This value ranges between 10 and 600 milliseconds. Window size should be greater than threshold count.

ethernet-oam link-monitor frame window <size(10-600)>

Mode Interface Configuration Mode(Physical)

Package Workgroup, Enterprise and Metro

Defaults 10 milliseconds

Example `iss(config-if)# ethernet-oam link-monitor frame window 200`

**Related
Commands**

- **show port ethernet-oam** - Displays EOAM local information
- **shutdown ethernet-oam** - Shutdown EOAM in all the ports of the the system and releases the allocated resources.

59.14 ethernet-oam link-monitor frame-sec-summary window

This command sets the window size for frame second summary. Window size must be greater than the threshold count. The window size ranges between 100 and 9000.. The no form of this command sets the window size for frame second summary to its default value.



The no form of this command is a subset of the combined form of the command for configuring the window and threshold parameters for the various types of link events.

```
ethernet-oam link-monitor frame-sec-summary window <size(100-9000)>
```

```
no ethernet-oam link-monitor {symbol-period | frame | frame-period | frame-sec-summary} {threshold | window}
```

Syntax Description	symbol-period	- Sends an event notification OAMPDU when an errored symbol period event occurs and the EOAM link event(s) supports the monitoring functionality in the switch.
	frame	- Sends an event notification OAMPDU when an errored frame event occurs.
	frame-period	- Sends an event notification OAMPDU when an errored frame period event occurs
	frame-sec-summary	- Sends an event notification OAMPDU when an errored frame period summary event occurs. Frame second summary window can be configured in both decimal and hexadecimal units.
	threshold	- Sets the the number of symbol errors that must occur within a given Window for generating an Event notification OAMPDU.
	window	- Sets the number of symbols (millions) over which the threshold event is defined.

Mode Interface Configuration Mode(Physical)

Package Workgroup, Enterprise and Metro

Defaults 100millisecond

Example

```
iss(config-if)# ethernet-oam link-monitor frame-sec-summary window 200
```



This command executes only if ethernet oam is not set as shutdown.

Related Commands

- **show port ethernet-oam** - Displays EOAM local information
- **shutdown ethernet-oam** - Shutdowns EOAM in all the ports of the the system and releases the allocated resources.

59.15 ethernet-oam link-monitor – threshold error count

This command sets the threshold error count for link monitoring. Threshold count must be lesser than window size for symbol-period and frame-period.

The no form of this command sets the threshold error count to its default value.



The no form of this command is a subset of the combined form of the command for configuring the window and threshold parameters for the various types of link events.

```
ethernet-oam link-monitor {symbol-period | frame | frame-period} threshold
<count (0xffff../1234..) >
```

```
no ethernet-oam link-monitor {symbol-period | frame | frame-period | frame-
sec-summary} {threshold | window}
```

Syntax Description	symbol-period	- Sends an event notification OAMPDU when an errored symbol period event occurs and the EOAM link event(s) supports the monitoring functionality in the switch.
	frame	- Sends an event notification OAMPDU when an errored frame event occurs.
	frame-period	- Sends an event notification OAMPDU when an errored frame period event occurs
	threshold <count (0xffff../1234..) >	- Sets the the number of symbol errors that must occur within a given Window for generating an Event notification OAMPDU.
	frame-period	- Sends an event notification OAMPDU when an errored frame period event occurs
	frame-sec-summary	- Sends an event notification OAMPDU when an errored frame period summary event occurs
	threshold	- Sets the the number of symbol errors that must occur within a given Window for generating an Event notification OAMPDU. The threshold value must not exceed the configured window size. This is not applicable for “frame” event.
	window	- Sets the number of symbols (millions) over which the threshold event is defined.
Mode	Interface Configuration Mode(Physical)	

Package Workgroup, Enterprise and Metro

Defaults symbol-period = 1

frame = 1

frame-period = 1

Example `iss(config-if)# ethernet-oam link-monitor frame threshold 5`



This command executes only if ethernet oam is not set as shutdown.

**Related
Commands**

- **show port ethernet-oam** - Displays EOAM local information
- **shutdown ethernet-oam** - Shutdown EOAM in all the ports of the the system and releases the allocated resources.

59.16 ethernet-oam link-monitor frame-sec-summary threshold

This command sets the threshold error count for frame seconds summary. Threshold error count for frame seconds summary must be lesser than the window size. The value ranges between 0 and 900.

The no form of this command sets the threshold error count to its default value.



The no form of the command is a subset of the combined form of the command for configuring the window and threshold parameters for the various types of link events.

```
ethernet-oam link-monitor frame-sec-summary threshold <count (0-900)>
```

```
no ethernet-oam link-monitor {symbol-period | frame | frame-period | frame-sec-summary} {threshold | window}
```

Syntax Description	symbol-period	- Sends an event notification OAMPDU when an errored symbol period event occurs and the EOAM link event(s) supports the monitoring functionality in the switch.
	frame	- Sends an event notification OAMPDU when an errored frame event occurs.
	frame-period	- Sends an event notification OAMPDU when an errored frame period event occurs
	frame-sec-summary	- Sends an event notification OAMPDU when an errored frame period summary event occurs
	threshold	- Sets the the number of symbol errors that must occur within a given Window for generating an Event notification OAMPDU. The threshold value must not exceed the configured window size.
	window	- Sets the number of symbols (millions) over which the threshold event is defined.

Mode Interface Configuration Mode(Physical)

Package Workgroup, Enterprise and Metro

Defaults 1

Example

```
iss(config-if)# ethernet-oam link-monitor frame-sec-summary threshold 6
```



This command executes only if ethernet oam is not set as shutdown.

Related Commands

- **show port ethernet-oam** - Displays EOAM local information
- **shutdown ethernet-oam** - Shutdown EOAM in all the ports of the the system and releases the allocated resources.

59.17 ethernet-oam - critical-event / dying-gasp

This command enables/disables critical event or dying gasp fault indication.

ethernet-oam {critical-event | dying-gasp} {enable | disable}

Syntax Description	critical-event	- Indicates the critical event to the peer OAM entity.
	dying-gasp	- Indicates the dying gasp to the peer OAM entity
	enable	- Enables the fault indication to the OAM entity
	disable	- Disables the fault indication to the OAM entity

Mode Interface Configuration Mode(Physical)

Package Workgroup, Enterprise and Metro

Defaults Enabled

Example `iss(config-if)# ethernet-oam critical-event enable`



This command executes only if ethernet oam is not set as shutdown.

- Related Commands**
- **show port ethernet-oam - event-log** - Displays EOAM event log
 - **shutdown ethernet-oam** - Shutdowns EOAM in all the ports of the system and releases the allocated resources.

59.18 clear port ethernet-oam - statistics

This command clears ethernet OAM configuration or statistics for all ports/specific port.

```
clear port ethernet-oam [<interface-type> <interface-id>] [statistics]
```

Syntax Description	<interface-type>	<ul style="list-style-type: none"> - Sets for the specified type of interface. The interface can be: <ul style="list-style-type: none"> • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
	<interface-id>	<ul style="list-style-type: none"> - Sets for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID
	statistics	<ul style="list-style-type: none"> - Sets the management information applicable to all the interfaces available in the switch.
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	
Example	iss# clear port ethernet-oam gigabitethernet 0/1	



- **clear port ethernet-oam** [<interface-type> <interface-id>] without the optional parameter **statistics** sets the port related configurable parameters of EOAM to their default values.
- **clear port ethernet-oam statistics** clears all the counters and gets incremented consistently if EOAM is enabled on the interface.
- This command executes only if ethernet oam is not set as shutdown.


**Related
Commands**

- **show port ethernet-oam** - Displays EOAM local information
- **show port ethernet-oam - statistics** - Displays EOAM statistics
- **shutdown ethernet-oam** - Shutdown EOAM in all the ports of the the system and releases the allocated resources.

59.19 clear port ethernet-oam – event log

This command clears the EOAM event log. If executed without the optional parameter this command clears the EOAM event log of all the interfaces.

```
clear port ethernet-oam [<interface-type> <interface-id>] event-log
```

Syntax Description	<interface-type>	-	Sets for the specified type of interface. The interface can be: <ul style="list-style-type: none"> • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
	<interface-id>	-	Sets-for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID
	event-log		Clears the event logs of all the ports.
Mode	Privileged EXEC Mode		
Package	Workgroup, Enterprise and Metro		
Example	iss# clear port ethernet-oam gigabitethernet 0/1 event-log		
	This command executes only if ethernet oam is not set as shutdown.		

**Related
Commands**

- **show port ethernet-oam - event-log** - Displays EOAM event log
- **shutdown ethernet-oam** - Shutdowns EOAM in all the ports of the the system and releases the allocated resources.

59.20 show ethernet-oam global information

This command displays the EOAM global configuration information.

show ethernet-oam global information

Mode Privileged EXEC Mode

Package Workgroup

Example iss# show ethernet-oam global information

```
Ethernet OAM has been enabled  
OUI configured is 00:01:02  
Error event OAMPDU resend count:10
```

**Related
Commands**

- **shutdown ethernet-oam** - Shutdowns EOAM in all the ports of the the system and releases the allocated resources.
- **set ethernet-oam** - Enables or disables EOAM in the system
- **set ethernet-oam oui** - Configures OUI
- **ethernet-oam link-monitor event-resend** - Sets the resend count of OAMPDU's to be sent for Event Notification

59.21 show port ethernet-oam

This command displays the EOAM local information.

show port ethernet-oam [<interface-type> <interface-id>]

Syntax	<interface-type>	- Displays for the specified type of interface. The interface can be:
Description		<ul style="list-style-type: none"> • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
	<interface-id>	<ul style="list-style-type: none"> - Displays for the specified interface identifier. This is a unique value that represents the specific interface. <p>This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel.</p> <p>For example: 0/1 represents that the slot number is 0 and port number is 1.</p> <p>Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID</p>
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	

Example iss# show port ethernet-oam gigabitethernet 0/1

Port	State	Mode	Status	Link Monitor	Config Rev	MaxPdu
-----	-----	-----	-----	-----	-----	-----
Gi0/1	enable	active	Operational	enable	2	90

Port	Remote Loopback	Link Event	UniDir	Variable retrieval
-----	-----	-----	-----	-----

```

-----
Gi0/1  deny      enable  disable enable

Port      ErrSymbol Period      ErrSymbol Period
          Window          Threshold
          (millions)      Count
-----
Gi0/1     18446744073709    1234

Port      ErrFrame Period  ErrFrame Period
          Window      Threshold
          Count
-----
Gi0/1     10000000        1

Port      Errored Frame      Errored Frame
          Window        Threshold
          (100 msec)    Count
-----
Gi0/1     1000          1

Port      ErrFrameSec Summary ErrFrameSec Summary
          Window          Threshold
          (100 msec)      Count
-----
Gi0/1     500          1

```



This command executes only if ethernet oam is not set as shutdown.

Related Commands

- **ethernet-oam** - Enables or disables EOAM on a port
- **ethernet-oam mode** - Configures the EOAM mode as either active or passive
- **ethernet-oam remote-loopback - deny/permit** - Ignores or processes the EOAM loopback commands
- **ethernet-oam link-monitor - link events** - Enables or disables EOAM link event(s) monitoring
- **ethernet-oam link-monitor - window size** - Sets the window size for EOAM link event monitoring
- **ethernet-oam link-monitor frame window** - Specifies the window size for the frame
- **ethernet-oam link-monitor frame-sec-summary window** - Sets the window size for frame second summary
- **ethernet-oam link-monitor - threshold error count** - Sets the threshold error count for link monitoring
- **ethernet-oam link-monitor frame-sec-summary threshold** - Sets the threshold error count for frame seconds summary
- **shutdown ethernet-oam** - Shutdown EOAM in all the ports of the the system and releases the allocated resources.

59.22 show port ethernet-oam - neighbor

This command displays EOAM local information of the neighbour. If executed without the optional parameters this command displays the EOAM peer information of all the available interfaces.

show port ethernet-oam [<interface-type> <interface-id>] neighbor

Syntax Description		
	<interface-type>	- Displays for the specified type of interface. The interface can be: <ul style="list-style-type: none"> • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
	<interface-id>	- Displays for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID
	neighbor	- Represents the adjacent module connected to the EOAM module.
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	

Example

```
iss# show port ethernet-oam gigabitethernet 0/1 neighbor
```

Port	Mac Addr	OUI	Vendor Info	Mode	Config Rev	Max Pdu
Gi0/1	00:02:02:03:04:01	00:02:02	00000000	active	1	90

Port	Remote Loopback	Link Event	UniDir	Variable retrieval
Gi0/1	enable	enable	disable	enable

Related Commands

- **shutdown ethernet-oam** - Shutdown EOAM in all the ports of the the system and releases the allocated resources.

59.23 show port ethernet-oam - loopback-capabilities

This command displays the EOAM information of the loopback capabilities. If executed without the optional parameters this command displays the EOAM loopback capabilities of all the available interfaces.

show port ethernet-oam [<interface-type> <interface-id>] loopback-capabilities

Syntax Description	<interface-type>	<ul style="list-style-type: none"> - Displays for the specified type of interface. The interface can be: <ul style="list-style-type: none"> • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
	<interface-id>	<ul style="list-style-type: none"> - Displays for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID
	loopback-capabilities	<ul style="list-style-type: none"> - Displays the EOAM information about the loopback capabilities.
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	

Example `iss# show port ethernet-oam gigabitethernet 0/1 loopback-`
`capabilities`

```
Remote Loopback
Port      Capability Control
-----
Gi0/1     enable          permit
```

**Related
Command**

- **ethernet-oam remote-loopback - deny/permit** - Ignores or processes the EOAM loopback commands
- **shutdown ethernet-oam** - Shutdown EOAM in all the ports of the the system and releases the allocated resources.

59.24 show port ethernet-oam - statistics

This command displays the EOAM statistics related information.

If executed without the optional parameters this command displays the EOAM statistics of all the available interfaces.

show port ethernet-oam [<interface-type> <interface-id>] statistics

Syntax Description	<interface-type>	<ul style="list-style-type: none"> - Displays for the specified type of interface. The interface can be: <ul style="list-style-type: none"> • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
	<interface-id>	<ul style="list-style-type: none"> - Displays for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID
	statistics	<ul style="list-style-type: none"> - Displays the statistics of all the ports.
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	
Example	iss# show port ethernet-oam gigabitethernet 0/1 statistics	

Port	InfoPduRx	UniEventRx	DupEventRx	RLBCtrlRx	VarReqRx	VarResRx
Gi0/1	30	0	0	0	0	0

Port	InfoPduTx	UniEventTx	DupEventTx	RLBCtrlTx	VarReqTx	VarResTx
Gi0/1	32	0	0	0	0	0

Port	OrgSpecRx	UnknownRx	OrgSpecTx	UnknownTx	FramesLost
Gi0/1	1	1	0	0	0

Related Command

- **clear port ethernet-oam - statistics** - Clears EOAM statistics and configuration
- **shutdown ethernet-oam** - Shutdown EOAM in all the ports of the the system and releases the allocated resources.

59.25 show port ethernet-oam - event-log

This command displays the EOAM event log.

If executed without the optional parameters this command displays the EOAM event log of all the available interfaces.

show port ethernet-oam [<interface-type> <interface-id>] event-log

Syntax	<interface-type>	<ul style="list-style-type: none"> - Displays for the specified type of interface. The interface can be: <ul style="list-style-type: none"> • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
Description	<interface-id>	<ul style="list-style-type: none"> - Displays for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID
	event-log	<ul style="list-style-type: none"> - Displays all the events logged for all the interfaces.
Mode	Privileged EXEC Mode	
Package	Workgroup	

Example `iss# show port ethernet-oam gigabitethernet 0/1 event-log`

```
Port: Gi0/1
Event: 1
      Time           : 7274
      OUI             : 00:03:02
      Event Type      : Errored Frame Event
      Location        : Local
      Window          : High: 0                      Low: 10
      Threshold       : High: 0                      Low: 1
      Value           : High: 0                      Low: 20
      Running Total   : High: 0                      Low: 20
      Event Total     : 1
Event: 2
      Time           : 24759
      OUI             : 01:80:c2
      Event Type      : Critical Link Event
      Location        : Local
Event: 3
      Time           : 24767
      OUI             : 01:80:c2
      Event Type      : Dying Gasp Event
      Location        : Local
Event: 4
      Time           : 24895
      OUI             : 01:80:c2
      Event Type      : Link Fault Event
      Location        : Local
```

**Related
Commands**

- **ethernet-oam - critical-event / dying-gasp** - Enables/disables critical event or dying gasp fault indication
- **clear port ethernet-oam - event log** - Clears EOAM event log
- **shutdown ethernet-oam** - Shutdown EOAM in all the ports of the the system and releases the allocated resources.

Chapter

60

FM

The **Interface Masters FM** (Fault Management) Module is a portable implementation of the Fault Management Module with minimum requirements. Currently, it is designed to interface with the **Interface Masters EOAM** Module. This is a prototype model used for testing **Interface Masters EOAM** and not a full fledged implementation. It provides complete management capabilities using SNMP and CLI.

Interface Masters FM supports the following features:

- Detect Link Fault, dying gasp and critical event conditions from the hardware and report it to **Interface Masters EOAM** module so that it can send notifications to the remote peer.
- FM module can request the EOAM module to send MIB variable requests on a particular interface.
- Registers itself with **Interface Masters EOAM** to receive Link events including Link fault, Dying gasp, Critical events, Event Notification OAMPDUs, Variable responses and Organization specific OAMPDUs from the remote peer.
- On reception of such events, the FM module sends a syslog message to log the event.
- **Interface Masters FM** also receives notifications when the remote peer is in loopback mode.
- When in remote loopback mode, the FM module can initiate remote loopback test to verify the link status.

The list of CLI commands for the configuration of FM is as follows:

- set fault-management
- fault-management ethernet-oam remote-loopback
- fault-management ethernet-oam link-monitor
- fault-management ethernet-oam

ISS

- fault-management ethernet-oam mib-variable count
- set fault-management ethernet-oam mib-request
- clear port fault-management ethernet-oam
- shutdown fault-management
- debug fault-management
- show fault-management global information
- show port fault-management eoam – MIB Variable Response
- show port fault-management ethernet-oam
- show port fault-management ethernet-oam – remote loopback

60.1 set fault-management

This command enables/disables fault management in the system. When enabled it detects link faults, dying gasp and critical events. The resources are allocated for the FM module,

```
set fault-management {enable | disable}
```

Syntax Description	enable	- Configures the Fault Management module as enabled on all the ports on the switch.
	disable	- Configures the Fault Management module as disabled on all ports on the switch.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults disable

Example `iss(config)# set fault-management enable`



The global admin status of the Fault Management Module must be UP.

Related Commands

- **no shutdown fault-management** - Starts fault management in the system
- **show fault-management global information** - Displays fault-management global information

60.2 fault-management ethernet-oam remote-loopback

This command specifies the number of packets and packet size for performing Ethernet OAM loopback test. This command also triggers the loop back test.

```
fault-management ethernet-oam remote-loopback ([test] [count <no of packets (1-1000)>] [packet <size (64-1500)>] [pattern <hex_string(8)>] [wait-time <integer (1-10)>])
```

Syntax Description	test	-	Initiates Loopback Test process
	count <no of packets (1-1000)>	-	Configures the number of packets to be sent for the loopback test. This value ranges between 1-1000.
	packet <size (64-1500)>	-	Configures the size of the test packets to be sent. The value ranges between 64-1500.
	pattern <hex_string(8)>	-	Configures the pattern of the Loopback Test data to be sent. This field is an octet string with size of 4. For example, 0xF0F0F0F0
	wait-time <integer (1-10)>	-	Configures the time until which the FM module waits for the reception of loopback test data. The value ranges between 1-10 seconds.

Mode Interface Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults	count	-	10
	packet size	-	64
	pattern	-	0xF0F0F0F0
	wait-time	-	5 seconds

Example

```
iss(config-if)# fault-management ethernet-oam remote-loopback test
```



- Interface admin status must be up
- Ethernet OAM must be enabled on the specified interface
- The global admin status of the Fault Management Module must be up
- Fault Management Module must be enabled

**Related
Commands**

- **no shutdown fault-management** - Starts fault management in the system
- **set fault-management** - Enables/disables fault management in the system

60.3 fault-management ethernet-oam link-monitor

This command configures the action to be taken for each EOAM link event described in the link event table for all the ports available in the switch.

```
fault-management ethernet-oam link-monitor {symbol-period | frame | frame-
period | frame-sec-summary} action {none | warning}
```

Syntax Description	symbol-period	-	Configures the symbol period event notification. The Errored Symbol Period Event is generated when the number of symbol errors exceeds a threshold within a configured value defined by a number of symbols.
	frame	-	Configures the frame event notification. The frame event is generated when the number of frame errors exceeds a threshold within a configured value defined by a period of time.
	frame-period	-	Configures the frame-period event notification. Frame period event is generated when the number of frame errors exceeds a threshold within a configured value defined by a number of frames
	frame-sec-summary	-	Configures the frame-seconds summary event notification. Frame Seconds Event is generated when the number of errored frame seconds exceeds a threshold within a configured value defined by time period. The errored frame second is defined as a one second interval that has at least one frame error.
	action	-	Action to be taken when a particular event is received none: no action will be taken when an event is received warning: a syslog message will be generated when an event is received
Mode	Interface Configuration Mode		
Package	Metro		
Defaults	action – warning for all events		

Example `iss(config-if)# fault-management ethernet-oam link-monitor
symbol-period action none`



The global administrative status of Fault Management Module must be up.

**Related
Commands**

- **no shutdown fault-management** - Starts fault management in the system
- **show port fault-management ethernet-oam** - Displays EOAM link event actions and max descriptors per variable request

60.4 fault-management ethernet-oam

This command configures action to be taken when a event (critical-event / dying-gasp / link-fault) occurs at the local interface and notification is received from remote interface. The associated action for that event is configured.

```
fault-management ethernet-oam {critical-event | dying-gasp | link-fault}
action {none | warning}
```

Syntax Description	critical-event	-	Configures the critical event fault indication received from local switch. Indicates the critical event through OAMPDU flags to its peer OAM entity.
	dying-gasp	-	Configures the dying gasp fault indication. Indicates a dying gasp event through the OAMPDU flags to its peer OAM entity.
	link-fault	-	Configures the link-fault indication. The link transmits OAMPDUs with a link-fault indication.
	action	-	Action to be taken when a particular event is received none: no action is taken when an event is received warning: a syslog message is generated when an event is received

Mode Interface Configuration Mode

Package Metro

Defaults action – warning for all events

Example

```
iss(config-if)# fault-management ethernet-oam critical-event
action none
```



The global administrative status of Fault Management Module must be up.

Related Commands

- no shutdown fault-management** - Starts fault management in the system
- show port fault-management ethernet-oam** - Displays EOAM link event actions and max descriptors per variable request

60.5 fault-management ethernet-oam mib-variable count

This command sets the maximum MIB variables that can be sent in one OAM variable request PDU.

fault-management ethernet-oam mib-variable count <count (1-100)>

Syntax Description	count<count (1-100)>	- MIB variable count
---------------------------	-----------------------------------	----------------------

Mode	Interface Configuration Mode
-------------	------------------------------

Package	Metro
----------------	-------

Defaults	10
-----------------	----

Example	<pre>iss(config-if)# fault-management ethernet-oam mib-variable count 50</pre>
----------------	--



The global administrative status of Fault Management Module must be up.

Related Commands	no shutdown fault-management - Starts fault management in the system
-------------------------	---

60.6 set fault-management ethernet-oam mib-request

This command configures the MIB variable string that is sent on the OAMPDU request to the peer.

```
set fault-management ethernet-oam mib-request <branch1leaf1:branch2leaf2:...>
```

Syntax Description **<branch1leaf1:branch2leaf2>** - Variable descriptor string that will be sent in the Variable Request OAMPDU.
 The format of the string must be 'branch1leaf1:branch2leaf2:...', where 'branch1' implies CMIP Branch1 (one-byte) 'leaf1' implies CMIP Leaf1 (two bytes) and similarly for other branches

Mode Interface Configuration Mode

Package Metro

Example `iss(config-if)# set fault-management ethernet-oam mib-request 74:75:76`



- The global administrative status of Fault Management Module must be up.
- EOAM must have been started and enabled.

Related Commands


- **no shutdown fault-management** - Starts fault management in the system
- **set fault-management** - Enables/disables fault management in the system
- **fault-management ethernet-oam mib-variable count** - Sets the maximum MIB variables that can be sent in one OAM variable request PDU
- **show port fault-management eoam - MIB Variable Response** - Displays MIB variable response

60.7 clear port fault-management ethernet-oam

This command clears MIB variable response received from the peer.

```
clear port fault-management ethernet-oam [<interface-type> <interface-id>]
mib-variable response
```

Syntax	<interface-type>	<ul style="list-style-type: none"> - Configures the specified type of interface. The interface can be: <ul style="list-style-type: none"> • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
Description	<interface-id>	<ul style="list-style-type: none"> - Configures the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.
	mib-variable response	<ul style="list-style-type: none"> - Denotes the mib variable response from the peer
Mode	Privileged Exec Mode	

Package	Workgroup, Enterprise and Metro
Example	<pre>iss# clear port fault-management ethernet-oam gigabitethernet 0/1 mib-variable response</pre>
	<ul style="list-style-type: none">The global administrative status of Fault Management Module must be up.
Related Commands	<ul style="list-style-type: none"><code>no shutdown fault-management</code> - Starts fault management in the system<code>show port fault-management eoam - MIB Variable Response</code> - Displays MIB variable response

60.8 shutdown fault-management

This command shuts down fault-management in the system and releases the allocated resources back to the system. The no form of the command starts fault management in the system.

shutdown fault-management

no shutdown fault-management

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# shutdown fault-management`

Related Commands `show fault-management global information` - Displays fault-management global information

60.9 debug fault-management

This command configures the debug trace level for FM module. When no parameters are given, this command displays the current debug level. The events failures and errors are captured using these statements. The statements are generated when the corresponding event occurs. The no form of the command disables debug option for the FM module. The debug statements are used to track the performance of Fault management module.

```
debug fault-management [all] [init] [mgmt] [critical] [pkt] [failure] [buffer]
[resource] [loopback] [event-trig] [event-rx] [var-reqresp] [ctrl] [func-
entry] [func-exit]
```

```
no debug fault-management {[all] | [init] [mgmt] [critical] [pkt] [failure]
[buffer] [resource] [loopback] [event-trig] [event-rx] [var-reqresp] [ctrl]
[func-entry] [func-exit]}
```

Syntax Description	all	-	Generates debug statements for all types of traces
	init	-	Generates debug statements for Init and shutdown Traces
	mgmt	-	Generates debug statements for management plane functionality traces
	critical	-	Generates traces messages for critical errors which need immediate attention.
	pkt	-	Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets
	failure	-	Generates trace messages for all types of failures
	buffer	-	Generates debug statements for traces with respect to allocation and freeing of Buffer.
	resource	-	Generates debug statements for Traces with respect to allocation and freeing of all resource except the buffers
	loopback	-	Generates debug statements when remote loopback test is requested.
	event-trig	-	Generates debug statements for fault event trigger traces.
	event-rx	-	Generates debug statements for event reception traces

	var-reqresp	-	Generates debug statements when mib variable request is sent or response is received on the interface.
	ctrl	-	Generates debug statements for Control Plane functionality traces
	func-entry	-	Generates trace messages for all functions entered in the module.
	func-exit	-	Generates trace messages for all the functions exited
Mode	Privileged Exec Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	critical		
Example	<pre>iss# debug fault-management init</pre>		
Related Commands	show debugging- Displays state of each debugging option		

60.10 show fault-management global information

This command displays fault-management global information. The status of the fault-management module is displayed.

show fault-management global information

Mode Privileged Exec Mode

Package Workgroup, Enterprise and Metro

Example iss# show fault-management global information

Fault-management module has been enabled

Related Commands **set fault-management** - Enables/disables fault management in the system

60.11 show port fault-management eoam – MIB Variable Response

This command displays MIB variable response on the port. The details such as MIB variable response number, branch, leaf width and so on.

show port fault-management ethernet-oam [<interface-type> <interface-id>] mib-variable response

Syntax Description	<interface-type>	- Displays the specified type of interface. The interface can be: <ul style="list-style-type: none"> • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
	<interface-id>	- Displays the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.
Mode	Privileged Exec Mode	
Package	Workgroup, Enterprise and Metro	
Example	<pre>iss# show port fault-management ethernet-oam gigabitethernet 0/2 mib-variable response</pre> <p>MIB variable responses received on interface gigabitethernet 0/2</p>	

MIB Variable response: 1

Branch	Leaf	Width/Indication	Value
07	00fb	04	00000014
07	00fc	04	00000013
07	00fe	04	00000000
07	00ff	04	00000000
07	0100	04	00000000
07	0101	04	00000000
07	0102	04	00000000
07	0103	04	00000001
07	0104	04	00000000
07	0105	04	00000000

MIB Variable response: 2

Branch	Leaf	Width/Indication	Value
07	0106	04	00000000

Related Commands **set fault-management ethernet-oam mib-request** - Sends MIB variable request to peer

60.12 show port fault-management ethernet-oam

This command displays EOAM link event actions and max descriptors per variable request.

```
show port fault-management ethernet-oam [<interface-type> <interface-id>]
```

Syntax Description	<interface-type>	<p>- Displays the specified type of interface. The interface can be:</p> <ul style="list-style-type: none"> • fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second. • gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links. • i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
	<interface-id>	<p>- Displays the specified interface identifier. This is a unique value that represents the specific interface.</p> <p>This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel.</p> <p>For example: 0/1 represents that the slot number is 0 and port number is 1.</p> <p>Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.</p>
Mode	Privileged Exec Mode	
Package	Workgroup, Enterprise and Metro	

Example `iss# show port fault-management ethernet-oam
gigabitethernet 0/1`

```

                                Link Event Action
-----
-----
Port Symbol Frame  Frame  Frame secs Critical Dying
Link MaxVar
      Period      Period Summary   Event   Gasp
Fault   /Req
-----
-----
Gi0/1 warning warning warning warning  warning
warning warning 10

```

**Related
Commands**

- **fault-management ethernet-oam link-monitor** - Specifies the action for the Link monitoring threshold crossing events received from local
- **fault-management ethernet-oam** - Specifies the action for the critical events received from local switch

60.13 show port fault-management ethernet-oam – remote loopback

This command displays Ethernet OAM loopback statistics. The information such as port number, loopback details, start date and end date are displayed.

```
show port fault-management ethernet-oam [<interface-type> <interface-id>]
remote-loopback {current-session | last-session} [detail]
```

Syntax Description

<interface-type>

- Displays the specified type of interface. The interface can be:
 - fastethernet – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.
 - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
 - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
 - i-lan / internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.
 - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.

<interface-id>

- Displays the specified interface identifier. This is a unique value that represents the specific interface.
This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel.
For example: 0/1 represents that the slot number is 0 and port number is 1.
Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

remote-loopback

- Displays the status of the remote-loopback for the current/previous session

	detail	- Displays detailed information about the current/last session of remote loopback.
Mode	Privileged Exec Mode	
Package	Workgroup, Enterprise and Metro	
Example	<pre>iss# show port fault-management ethernet-oam gigabitethernet 0/3 remote-loopback current-session detail Port: Gi0/3 Loopback: Remote OAM in loopback mode Start: Feb 12 12:51:08 2007 End: Still running Test pattern: f0f0f0f0 Test packet size: 64 Test wait-time: 5 Test packet count: 10 Test statistics: Test packets Rx: 10 Test packets Tx: 10 Test packets matched: 10</pre>	
Related Commands	fault-management ethernet-oam remote-loopback - Specifies the number of packets and packet size for performing Ethernet OAM loopback test	

Chapter

61

RM

Redundancy Manager (RM) is an implementation of 1:1 Warm Standby and Cold Standby Redundancy. It provides support for hot-swap. It is a portable software implementation of a framework for providing fault tolerance for software and firmware components in a system. Fault management becomes a critical task in systems where the downtime should be minimal. This demands a software that is engineered to work around hardware failures and handle software upgrades without the necessity to be restarted. **Interface Masters RM** is a solution to address this problem by providing a framework for software components to quickly add redundancy capability.

The list of CLI commands for the configuration of RM is as follows:

- redundancy
- hb-interval
- peer-dead-interval
- peer-dead-interval-multiplier
- redundancy force-switchover
- debug rmgr
- show redundancy

61.1 redundancy

This command allows to enter into the redundancy configuration mode.

redundancy

Mode Global Configuration Mode

Package Metro

Example `iss(config)# redundancy`

- Related Commands**
- **hb-interval** - Specifies the interval between Heart Beat messages
 - **peer-dead-interval** - Specifies the interval after which the peer node is declared as dead
 - **redundancy force-switchover** - Conducts a manual switchover from ACTIVE to STANDBY
 - **peer-dead-interval-multiplier** - Specifies the multiplier by which the heart beat interval is multiplied to get the peer dead interval.

61.2 hb-interval

This command specifies the interval (in milliseconds) between Heart Beat messages.

hb-interval <interval (10-5000)>

Mode Redundancy Configuration Mode

Package Metro

Defaults 1000 milliseconds

Example `iss (config-r)# hb-interval 2000`



- The Heart Beat Interval is the time interval between two Heart beat messages
- As a pre-requisite, the Peer Dead Interval value has to be configured four times greater than the Heart Beat Interval value
- This Heart Beat Interval value must be the same for all the nodes in the network
- This command can be executed only in active node

**Related
Commands**

- **peer-dead-interval** - Specifies the interval after which the peer node is declared as dead
- **show redundancy** - Displays the Redundancy Manager configuration details

61.3 peer-dead-interval

This command specifies the interval (in milliseconds) after which the peer node is declared as dead.

This CLI command is maintained only for backward compatibility. Peer dead interval multiplier command is used for configuring peer dead interval.

peer-dead-interval <interval(40-20000)>

Mode Redundancy Configuration Mode

Package Metro

Defaults 4000 milliseconds

Example `iss (config-r)# peer-dead-interval 8000`



- The Peer Dead Interval value has to be configured four times greater than the Heart Beat Interval value
- The Peer Dead Interval value must be the same for all the nodes in the network
- This command can be executed only in the active node

**Related
Commands**

- **hb-interval** - Specifies the interval between Heart Beat messages
- **show redundancy** - Displays the Redundancy Manager configuration details

61.4 peer-dead-interval-multiplier

This command specifies the multiplier by which the heart beat interval (in milliseconds) is multiplied to get the peer dead interval.

Peer Dead Interval = Heart Beat Interval * Peer Dead Interval Multiplier

peer-dead-interval-multiplier <interval(4-10)>

Mode Redundancy Configuration Mode

Package Metro

Defaults 4

Example iss (config-r)# peer-dead-interval-multiplier 5

Related Commands

- **hb-interval** - Specifies the interval between Heart Beat messages
- **show redundancy** - Displays the Redundancy Manager configuration details
- **peer-dead-interval** - Specifies the interval after which the peer node is declared as dead

61.5 redundancy force-switchover

This command conducts a manual switchover from ACTIVE to STANDBY.

redundancy force-switchover

Mode USER / Privileged EXEC Mode

Package Metro

Example iss# redundancy force-switchover



This command can be executed only in the active node.

Related Command **show redundancy** - Displays the Redundancy Manager configuration details

61.6 debug rmgr

This command enables debugging for the configured options. The no form of the command disables debugging for the configured points..

```
debug rmgr {all | critical | failure | state-machine | timer | socket | file-
transfer | snmp | notification | syncup-msg | buffer | event | dump-trc |
control-plane-trc | switchover }
```

```
no debug rmgr {all | critical | failure | state-machine | timer | socket |
file-transfer | snmp | notification | syncup-msg | buffer | event | dump-trc |
control-plane-trc | switchover }
```

Syntax	all	-	All Traces
	critical	-	Critical Traces
Description	failure	-	Failure Traces
	state-machine	-	State Machine Traces
	timer	-	Timer Traces
	socket	-	Socket Traces
	file-transfer	-	File Transfer Traces
	snmp	-	SNMP Related Traces
	notification	-	Notification Traces
	syncup-msg	-	Syncorization Message Traces
	Buffer		Buffer Traces
	Event		Event Traces
	dump-trc		Packet Dump Traces
	control-plane-trc		Control Plane Traces
	switchover	-	Switchover Traces

Mode USER / Privileged EXEC Mode

Package Metro

Defaults critical

Example iss# debug rmgr all

61.7 show redundancy

This command displays the Redundancy Manager configuration details.

show redundancy

Mode USER / Privileged EXEC Mode

Package Metro

Example iss# show redundancy

```
Redundancy Manager Configuration details
Self NodeId: 127.1.0.1
Peer NodeId: 127.1.0.2
Active NodeId: 127.1.0.1
Node Status: Active
HearBeat Interval: 1000 msec
Peer Dead Interval : 4000 msec
```

**Related
Commands**

- **hb-interval** - Specifies the interval between Heart Beat messages
- **peer-dead-interval** - Specifies the interval after which the peer node is declared as dead
- **redundancy force-switchover** - Conducts a manual switchover from ACTIVE to STANDBY

Chapter

62

PTP

Interface Masters PTP (Precision Time Protocol) is a stand alone software which implements IEEE 1588, a standard that describes about synchronization of clocks of measurement and control applications using distributed system technologies. PTP is a message based protocol which specifies how the real-time clocks in the system in distributed system synchronize with each other. PTP creates master-slave hierarchy to synchronize the clocks in the system.

The list of CLI commands for the configuration of PTP is as follows:

- shutdown ptp
- ptp - vrf | switch
- ptp enable | disable
- ptp primary-context
- ptp notification
- ptp primary-domain
- ptp two-step-clock
- ptp clock ports
- ptp port
- ptp mode
- ptp slave
- ptp pathtrace
- ptp alternate-time-scale key
- ptp alternate-time-scale enable key

- ptp alternate-time-scale key
- ptp acceptable-master protocol
- ptp alternate-master
- ptp acceptable-master enable
- ptp max alternate-masters
- show ptp global info
- show ptp vrf | switch info
- show ptp clock
- show ptp foreign-master-record
- show ptp parent
- show ptp port
- show ptp counters
- show ptp time-property
- show ptp current
- show ptp acceptable masters
- show ptp alternate time-scale
- debug ptp
- ptp
- ptp - ipv6
- ptp alternate-master - ipv6
- ptp acceptable-master enable - ipv6
- ptp max alternate-masters - ipv6

62.1 shutdown ptp

This command shuts down PTP in the device. This removes all the PTP related configurations, such as domain, port, clock and other related information, from the system. The no form of the command starts PTP in the device. This allows the user to configure the PTP parameters. When started, PTP module initializes its global information. This includes creation of memory pools, queues and semaphores.

shutdown ptp

no shutdown ptp

Mode	Global Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	PTP is shutdown.
Example	<code>iss(config)# no shutdown ptp</code>
Related Command	<code>show ptp global info</code> - Displays the PTP clock global information.

62.2 ptp - vrf | switch

This command creates a PTP domain in a virtual context. If no virtual context / domain is specified, default context / domain will be configured. The no form of the command deletes a PTP domain in a virtual context. If no virtual context / domain is specified, default domain / context will be deleted.

```
ptp [{ vrf | switch } <context-name>] [domain <id (0-127)>]
```

```
no ptp [{ vrf | switch } <context-name>] [domain <short (0-127)>]
```

Syntax Description	vrf	- Name of the VRF instance. This value is a string of size 32.
	switch	- Name of the switch context. This value is a string of size 32.
	context-name	- 32-bit unique context identifier. Each virtual context will be able to run PTP individually and this distinguishes multiple virtual contexts present in the switch/router. This value ranges between 0 and 255.
	domain	- Unique identifier of the domain. This domain ID defines the scope of the PTP message communication, state, operations, data sets and timescale. This value ranges between 0 and 255.
		- 0 Default domain - 1 to 3 Alternate domains - 128 to 255 Reserved
defaults	Default domain is 0	
Mode	Global Configuration Mode	
Package	Workgroup, Enterprise and Metro	
Example	iss(config)# ptp vrf default domain 0	
	iss(config)# ptp switch default domain 0	
Related Command	show ptp vrf switch info - Displays the PTP clock information for a context.	

62.3 ptp enable | disable

This command enables PTP in a virtual context. If virtual context is not specified, default context will be configured. The no form of the command disables PTP in a virtual context. When PTP is disabled, the PTP will be non operational in the virtual context. The resources alone will be reserved for the functioning of the PTP.

```
ptp enable [{ vrf | switch } <context-name>]
```

```
ptp disable [{ vrf | switch } <context-name>]
```

Syntax Description	vrf	- Name of the VRF instance. This value is a string of size 32.
	switch	- Name of the switch context. This value is a string of size 32.
	context-name	- 32-bit unique context identifier. Each virtual context will be able to run PTP individually and this distinguishes multiple virtual contexts present in the switch/router. This value ranges between 0 and 255.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults PTP is disabled in the virtual context.

Example

```
iss(config)# ptp enable switch sw1
iss(config)# ptp enable vrf default
```



Before the PTP is enabled, the clock type (one-step or two -step) should be configured. If there is any change, then the same will reflect only when the module is disabled and enabled again.

Related Command **show ptp vrf | switch info** - Displays the PTP clock information for a context.

62.4 ptp primary-context

This command configures the PTP primary context, which configures the system clock. This value ranges between 0 and 255. By default, this is configured to the default context ID (0).

The administrator should explicitly configure the context. If the primary context is deleted, the user has to explicitly configure a new primary context.

```
ptp primary-context { vrf | switch } <context-name>
```

Syntax Description	vrf	- Name of the VRF instance. This value is a string of size 32.
	switch	- Name of the switch context. This value is a string of size 32.
	context-name	- 32-bit unique context identifier. Each virtual context will be able to run PTP individually and this distinguishes multiple virtual contexts present in the switch/router. This value ranges between 0 and 255.

Mode Global Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config)# ptp primary-context vrf text`

62.5 ptp notification

This command enables trap for notifying the PTP failures and state changes. The no form of the command disables trap set for notifying PTP failures or state changes.

```
ptp notification {[global-error] [sys-ctrl-change] [sys-admin-change] [port-
state-change] [port-admin-change] [sync-fault] [gm-fault] [acc-master-fault]
[unicast-admin-change]}
```

```
no ptp notification {[global-error] [sys-ctrl-change] [sys-admin-change]
[port-state-change] [port-admin-change] [sync-fault] [gm-fault] [acc-master-
fault] [unicast-admin-change]}
```

Syntax Description	global-error	-	Generated whenever any of the error events such as memory allocation failure or buffer allocation failure occur in PTP. The generated trap carries the information about the type of the resource allocation failure (memory allocation or buffer allocation).
	sys-ctrl-change	-	Generated whenever PTP is shutdown or started in the context. The generated trap carries the information of the virtual context in which the PTP status is changed along with the system control status (Start/Shutdown).
	sys-admin-change	-	Generated whenever PTP is enabled or disabled in the context. The generated trap carries the information of the virtual context in which the PTP status is changed along with the admin status (Enabled/Disabled).
	port-state-change	-	Generated whenever a state change occurs for the PTP port. The generated trap carries, the context name in which the trap occurred and the newly selected port state. Context identifier, domain name and PTP port index trio form the index for the PTP port state and hence will be embedded along with this trap.
	port-admin-change	-	Generated whenever PTP is enabled or disabled in a port. The generated trap contains information about the context name of the port bound where the PTP status is changed. Context identifier and domain identifier along with the port will be embedded as indices of the PTP port status.

	sync-fault	- Generated whenever PTP synchronization fault occurs in the system. The generated trap contains the virtual context name, domain number along with the port where the fault occurred.
	gm-fault	- Generated whenever PTP grandmaster fault occurs in the system. The generated trap contains the virtual context name, domain number along with the port where the fault occurred.
	acc-master-fault	- Generated whenever PTP acceptable master fault occurs in the system. The generated trap contains the virtual context name, domain number along with the port where the fault occurred.
	unicast-admin-change	- Generated whenever PTP unicast option is enabled or disabled in the context. The generated trap contains the information about the context name of the port bound where the unicast negotiation option is changed.
Default	Notification is enabled	
Mode	Global Configuration Mode	
Package	Workgroup, Enterprise and Metro	
Example	<pre>iss(config)# ptp notification global-error sys-ctrl-change sys-admin-change port-state-change port-admin-change sync- fault gm-fault acc-master-fault</pre>	
Related Command	show ptp global info - Displays the PTP clock global information.	

62.6 ptp primary-domain

This command configures the current domain as PTP primary domain, which configures the system clock. This value ranges between 0 and 255. By default, this is configured to the default domain ID (0).

The administrator should explicitly configure the domain. If the primary domain is deleted, the user has to explicitly configure a new primary domain.

ptp primary-domain

Mode PTP Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 0

Example `iss(config-ptp)# ptp primary-domain`

Related Command `show ptp clock` - Displays the PTP clock properties of the given virtual switch and domain.

62.7 ptp two-step-clock

This command configures PTP clock as two step clock. Two-step clock provides time information using the combination of an event message and a subsequent general message. The no form of the command configures PTP clock as default one step clock. One-step clock provides time information using a single event message.

ptp two-step-clock

no ptp two-step-clock

Mode PTP Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults One step clock

Example `iss(config-ptp)# ptp two-step-clock`



This configuration can be done, only if the PTP domain row status is not in service.

Related Command **show ptp clock** - Displays the PTP clock properties of the given virtual switch and domain.

62.8 ptp clock ports

This command configures the number of PTP clock ports on the device. This value ranges between 0 and 255. For an ordinary clock, this value should be 1

ptp clock ports <number-of-ports>

Mode PTP Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults 0

Example iss(config-ptp)# ptp clock ports 2



This configuration can be done, only if the PTP domain row status is not in service.

Related Command **show ptp clock** - Displays the PTP clock properties of the given virtual switch and domain.

62.9 ptp port

This command adds port to the PTP clock. That is, specifies the type of the interface that the PTP runs over. PTP interfaces running in a node or system, interfaces with the network through entities called PTP ports. PTP ports are different from the set of interfaces defined in the interface MIB. The no form of the command deletes port from the PTP clock.

```
ptp port [{ ipv4 | ipv6 }] {<iftype> <ifindex> | vlan <index> [switch <switch-name>]}
```

```
no ptp port [{ ipv4 | ipv6 }] {<ifXtype> <ifnum> | vlan <integer> [switch <switch-name>]}
```

Syntax Description	ipv4	- Internet Protocol version 4.
	ipv6	- Internet Protocol version 6.
	iftype	- Ethernet interface type assigned in the interface manager of the system.
	ifindex	- Ethernet interface index number assigned in the interface manager of the system.
	vlan	- VLAN identifier assigned in the interface manager of the system.
	switch	- 32-bit unique context identifier. Each virtual context will be able to run PTP individually and this distinguishes multiple virtual contexts present in the switch/router. This value ranges between 0 and 255.

Mode PTP Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config-ptp)# ptp port vlan 3
iss(config-ptp)# ptp port ipv4 vlan 3
iss(config-ptp)# ptp port ipv6 vlan 3
```

Related Command

```
iss(config-ptp)# ptp port ipv4 gigabitethernet 0/1
```

show ptp port - Displays all the PTP port properties of the given virtual switch and domain.

62.10 ptp mode

This command configures PTP clock mode and clock priorities. PTP clock mode specifies the operating mode of the clock in the domain. Clock priorities are used by the BMC (Best Master Clock) algorithm to select the best master clock. The no form of the command sets PTP clock mode and clock priorities to default values.

```
ptp { mode { ordinary | boundary | e2ettransparent | p2pttransparent | forward }
| priority1 <value(0-255)> | priority2 <value(0-255)> }
```

```
no ptp { mode [{ordinary | boundary | e2ettransparent | p2pttransparent |
forward }] | priority1 [<value(0-255)>] | priority2 [<value(0-255)>] }
```

Syntax Description	ordinary	- Clock is in ordinary mode. Contains a single PTP port in a domain and maintains the timescale used in the domain. It may serve as a source of time, that is, a master clock, or may synchronize to another clock, that is, a slave clock.
	boundary	- Clock is in boundary mode. Contains multiple PTP ports in a domain and maintains the timescale used in the domain. It may serve as the source of time, that is, a master clock, and may synchronize to another clock, that is, a slave clock.
	e2ettransparent	- Clock is in end-to-end transparent mode. Measures the time taken for a PTP event message to transit the device and provides this information to clocks receiving this PTP event message.
	p2pttransparent	- Clock is in peer-to-peer transparent mode. Measures the time taken for a PTP event message to transit the device and provides this information to clocks receiving this PTP event message.
	forward	- Clock is in forwarding mode. Does not perform any PTP processing, just forwards the PTP messages on other ports.
	priority1	- Priority 1 value used by the BMC algorithm to select the best master clock. Lower values take higher precedence. This value ranges between 0 and 255.

priority2 - Priority 2 value used by the BMC algorithm to select the best master clock. This value is used as a tiebreaker when the BMC fails to order the clock using priority 1, clock class, clock accuracy and clock offset scaled log variance. Lower values take higher precedence.

This value ranges between 0 and 255.

Mode PTP Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults mode - forward

priority1 - 128

priority2 - 128

Example `iss(config-ptp)# ptp mode ordinary`

`iss(config-ptp)# ptp priority1 20`

Related Command

- **show ptp clock** - Displays the PTP clock properties of the given virtual switch and domain.
- **show ptp parent** - the parent and grand-master properties of the given virtual switch and domain.

62.11 ptp slave

This command configures the clock as a slave only clock. That is, the clock is synchronized to another clock. A boundary clock cannot be a slave only clock. The no form of the command configures the clock to default forward mode. That is, the clock is not synchronized to another clock.

ptp slave

no ptp slave

Mode PTP Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults The clock is not configured as a slave only clock.

Example `iss(config-ptp)# ptp slave`



The slave only option is applicable for ordinary clock only.

Related Command **show ptp clock** - Displays the PTP clock properties of the given virtual switch and domain.

62.12 ptp pathtrace

This command enables PTP pathtrace option in the system. Path trace is used to trace the route of a PTP announce message through the timing system in the boundary clocks and avoid the announce message looped in the timing system. The no form of the command disables PTP pathtrace option in the system. When path trace is disabled, the path trace TLV will not be presenting the PTP messages.

ptp pathtrace

no ptp pathtrace

Mode	PTP Configuration Mode
Package	Workgroup, Enterprise and Metro
Defaults	Pathtrace option is disabled.
Example	<code>iss(config-ptp)# ptp pathtrace</code>
Related Command	<code>show ptp clock</code> - Displays the PTP clock properties of the given virtual switch and domain.

62.13 ptp alternate-time-scale key

This command configures the alternate time scale that PTP grandmaster supports. This is used to indicate the offset of an alternate time from its node at the grandmaster clock. The unique identifier of the alternate timescale key identifier is used to identify the time scale offset. This value ranges between 1 and 254. The no form of the command deletes the alternate time scale that PTP grandmaster supports.

```
ptp alternate-time-scale key <value(0-254)> name <string(10)>
```

```
no ptp alternate-time-scale key <value(0-254)> name [<string(10)>]
```

Syntax Description	name	- Text name of the alternate timescale. Commonly used acronyms should be used, for example, NTP, PT, PST, PDT for Network Time Protocol, Pacific Time, Pacific Standard Time, and Pacific Daylight Savings Time, respectively. The maximum number of symbols is 10.
---------------------------	-------------	---

Mode	PTP Configuration Mode
-------------	------------------------

Package	Workgroup, Enterprise and Metro
----------------	---------------------------------

Example	iss(config-ptp)# ptp alternate-time-scale key 3 name NTP
----------------	--

Related Command	show ptp alternate time-scale - Displays PTP alternate timescale properties of the given virtual switch and domain.
------------------------	--

62.14 **ptp alternate-time-scale enable key**

This command enables PTP alternate time scale option. This is used to indicate the offset of an alternate time from its node at the grandmaster clock. The no form of the command disables PTP alternate time scale option.

```
ptp alternate-time-scale enable key <value(0-254)>
```

```
no ptp alternate-time-scale-enable key <value(0-254)>
```

Mode PTP Configuration Mode

Package Workgroup, Enterprise and Metro

Example `iss(config-ptp)# ptp alternate-time-scale enable key 1`

Related Command **show ptp alternate time-scale** - Displays PTP alternate timescale properties of the given virtual switch and domain.

62.15 ptp alternate-time-scale key

This command configures the PTP alternate time scale properties, current-offset, jump-seconds and next-jump in seconds. The no form of the command resets the alternate time scale properties.

```
ptp alternate-time-scale key <value(0-254)> [ current-offset <value>] [jump-seconds <value>] [next-jump <value>]
```

```
no ptp alternate-time-scale key <value(0-254)> [ current-offset <value>] [jump-seconds <value>] [next-jump <value>]
```

Syntax Description	current-offset	- The offset of the alternate time, in seconds, from the node time. The alternate time is the sum of this value and the node time.
	jump-seconds	- Size of the next discontinuity, in seconds, of the alternate time. A value of zero indicates that no discontinuity is expected. A positive value indicates that the discontinuity will cause the current offset of the alternate time to increase.
	next-jump	- The value of the seconds portion of the transmitting node time at the time that the next discontinuity will occur. The discontinuity occurs at the start of the second indicated by this value. The value of next-jump seconds can carry 48 bits.

Mode PTP Configuration Mode

Package Workgroup, Enterprise and Metro

Example

```
iss(config-ptp)# ptp alternate-time-scale key 1 current-  
offset 10 jump-seconds 20 next-jump 50
```

Related Command

- **show ptp alternate time-scale** - Displays PTP alternate timescale properties of the given virtual switch and domain.
- **show ptp current** - Displays PTP current offset and meanpath delay value with the master of the given virtual switch and domain.

62.16 ptp acceptable-master protocol

This command configures the PTP acceptable masters. Acceptable master table contains acceptable masters for the clock. This table allows the slave ports to refuse to synchronize to clocks not on the acceptable master list. The no form of the command deletes a configured PTP acceptable master.

```
ptp acceptable-master protocol { ipv4 <ip-address> | ipv6 <ip6-address> |
ethernet <mac-address>} [alternatePriority1 <0-255>]
```

```
no ptp acceptable-master protocol { ipv4 <ip-address> | ipv6 <ip-address> |
ethernet <ucast_mac> } [alternatePriority1 [<0-255>]]
```

Syntax Description	ipv4	- Internet Protocol version 4.
	ipv6	- Internet Protocol version 6.
	ethernet	- Ethernet interface.
	alternatePriority1	- Alternate priority value that replaces the priority1 of the clock set for selecting the best master algorithm. This value ranges between 0 and 255.

Mode PTP Configuration Mode

Package Workgroup, Enterprise and Metro

Example iss(config-ptp)# ptp acceptable-master protocol ipv4 10.0.0.1
alternatePriority1 50

```
iss(config-ptp)# ptp acceptable-master protocol ipv6
482f::4830 alternatePriority1 50
```

```
iss(config-ptp)# ptp acceptable-master protocol ethernet
00:80:30:FF:FE:10 alternatePriority1 50
```

Related Command **show ptp acceptable masters** - Displays PTP acceptable master information of the given virtual switch and domain.

62.17 ptp alternate-master

This command enables PTP alternate master option and configures alternate sync interval. This interval is set using log base 2 values. The no form of the command disables PTP alternate master option and resets the alternate sync interval to default values.

```
ptp alternate-master { alternate-multisync | multisync-interval <short (0-255)> } [domain <short (0-127)>]
```

```
no ptp alternate-master { alternate-multisync | multisync-interval <short (0-255)> } [domain <short (0-127)>]
```

Syntax Description	alternate-multisync	-	This is TRUE and if the port is transmitting multicast announce message with alternate master flag true, then the slave port can also transmit multicast sync messages with alternate master flag as true.		
	multisync-interval	-	Interval in seconds between the sync messages transmitted with alternate master flag as true. This value ranges between 0 and 255.		
	domain	-	Unique identifier of the domain. This domain ID defines the scope of the PTP message communication, state, operations, data sets and timescale. This value ranges between 0 and 255.		
			0	Default domain ID.	
			1 to 3	Alternate domains.	
			128 to 255	Reserved.	
Mode	Interface Configuration Mode				
Package	Workgroup, Enterprise and Metro				
Defaults	alternate-multisync	-	false		
	multisync-interval	-	0		
Example	<pre>iss(config-ptp)# ptp alternate-master alternate-multisync domain 2</pre>				
Related Command	show ptp port - Displays all the PTP port properties of the given virtual switch and domain.				

62.18 ptp acceptable-master enable

This command enables acceptable master option on port. Acceptable master option is used to allow slave ports to refuse to synchronize to clocks not on the acceptable master list. The no form of the command disables acceptable master option on port.

```
ptp acceptable-master enable [domain <short (0-127)>]
```

```
no ptp acceptable-master enable [domain <short (0-127)>]
```

Syntax Description	domain	-	Unique identifier of the domain. This domain ID defines the scope of the PTP message communication, state, operations, data sets and timescale. This value ranges between 0 and 255.
		0	Default domain ID.
		1 to 3	Alternate domains.
		128 to 255	Reserved.
Mode	Interface Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	Acceptable master option is disabled.		
Example	iss(config-ptp)# ptp acceptable-master enable domain 2		
Related Command	show ptp acceptable masters - Displays PTP acceptable master information of the given virtual switch and domain.		

62.19 ptp max alternate-masters

This command configures the number of alternate masters on this port. The number of alternate masters ranges between 0 and 255. The no form of the command resets the number of alternate masters on this port to default values.

```
ptp max alternate-masters <value(0-255)> [domain <short(0-127)>]
```

```
no ptp max alternate-masters [<integer(0-255)>] [domain <short(0-127)>]
```

Syntax Description	domain	-	Unique identifier of the domain. This domain ID defines the scope of the PTP message communication, state, operations, data sets and timescale. This value ranges between 0 and 255.
		0	Default domain ID.
		1 to 3	Alternate domains.
		128 to 255	Reserved.
Mode	Interface Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	Number of alternate masters is 0.		
Example	iss(config-ptp)# ptp max alternate-masters 10 domain 2		
Related Command	show ptp port - Displays all the PTP port properties of the given virtual switch and domain.		

62.20 ptp

This command configures PTP system parameters. The no form of the command configures PTP system parameters to default. Intervals are set using log base 2 values, that is, if announce interval is 0, it means 1 packet every second.

```
ptp {announce { interval <value(0-4)> | timeout <value(2-10)> } | delay-req
interval <value(0-5)> | enable | sync { interval <value(-1-1)> | limit
<value(50-1000000000)> } | delay mechanism <integer(1-2)> | version <value(1-
2)> } [domain <id (0-127)>]
```

```
no ptp { announce {interval [<value(0-4)>] | timeout [<value(2-10)>]} | delay-
req interval [<value(0-5)>] | enable | sync { interval [<value(-1-1)>] | limit
[<value(50-1000000000)>] } | delay mechanism [<value(1-2)>] | version
[<value(1-2)>] } [domain <id (0-127)>]
```

Syntax Description

- | | | |
|---------------------------|---|---|
| announce | - | Logarithm to the base 2 of the mean announce message interval in seconds. Announce message is used to form master-slave hierarchy. When a clock comes online, an ordinary clock or boundary clock listens for announce message from the master for a configurable time interval. If no announce message is received within this time, the clock assumes itself as the master, until a better clock appears.
This value ranges between 0 and 4. |
| timeout | - | Announce receipt time out value. When a clock comes online, an ordinary clock or boundary clock listens for announce message from the master for a configurable time interval. This time interval is the announce timeout value. This should be an integral multiple of announce interval in seconds.
This value ranges between 2 and 10. |
| delay-req interval | - | Time to the member devices to send delay request messages when the port is the master. This is the logarithm to the base 2 of the delay request interval in seconds.
This value ranges between 0 and 5. |
| enable | - | Enables PTP in the domain. |

	interval	-	Logarithm to the base 2 of the sync message interval in seconds. Sync message is the event message used for slave clock synchronization and will be time stamped. This value ranges between -1 and 1.
	limit	-	Maximum clock offset value before which the PTP attempts to resynchronize. This value ranges between 50 and 1000000000 nanoseconds.
	delay mechanism	-	Propagation delay measuring option used by the port in computing the mean path delay. Options are: 1 – End-to-end delay measurement mechanism between slave clocks and the master clock. 2 – Peer-to-peer delay measurement mechanism between slave clocks and the master clock.
	version	-	PTP version on which the PTP receive time stamp configuration is applicable. Options are: 1 – PTP version 1. 2 – PTP version 2.
	domain	-	Unique identifier of the domain. This domain ID defines the scope of the PTP message communication, state, operations, data sets and timescale. This value ranges between 0 and 255.
		0	Default domain ID.
		1 to 3	Alternate domains.
		128 to 255	Reserved.
Mode	Interface Configuration Mode / VLAN Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	announce	-	1
	timeout	-	3
	delay-req interval	-	0

interval	-	0
limit	-	1000000000 nanoseconds
delay mechanism	-	1
version	-	2

Example `iss(config-if)# ptp announce interval 2 domain 2`

Related Command

- **show ptp port** - Displays all the PTP port properties of the given virtual switch and domain.
- **show ptp foreign-master-record** - displays the PTP foreign-master information of the given virtual switch and domain.
- **show ptp counters** - Displays all the PTP port counters of the given virtual switch and domain.

62.21 ptp - ipv6

This command configures PTP system parameters. The no form of the command configures PTP system parameters to default. Intervals are set using log base 2 values, that is, if announce interval is 0, it means 1 packet every second.

```
ptp {announce { interval <value(0-4)> | timeout <value(2-10)> } | delay-req
interval <value(0-5)> | enable | sync { interval <value(-1-1)> | limit
<value(50-1000000000)> } | delay mechanism <integer(1-2)> | version <value(1-
2)> } [domain <id (0-127)>] [ ipv6 ]
```

```
no ptp { announce {interval [<value(0-4)>] | timeout [<value(2-10)>]} | delay-
req interval [<value(0-5)>] | enable |sync { interval [<value(-1-1)>] | limit
[<value(50-1000000000)>] } | delay mechanism [<value(1-2)>] | version
[<value(1-2)>]} [domain <id (0-127)>] [ ipv6 ]
```

Syntax Description

- | | | |
|---------------------------|---|---|
| announce | - | Logarithm to the base 2 of the mean announce message interval in seconds. Announce message is used to form master-slave hierarchy. When a clock comes online, an ordinary clock or boundary clock listens for announce message from the master for a configurable time interval. If no announce message is received within this time, the clock assumes itself as the master, until a better clock appears.
This value ranges between 0 and 4. |
| timeout | - | Announce receipt time out value. When a clock comes online, an ordinary clock or boundary clock listens for announce message from the master for a configurable time interval. This time interval is the announce timeout value. This should be an integral multiple of announce interval in seconds.
This value ranges between 2 and 10. |
| delay-req interval | - | Time to the member devices to send delay request messages when the port is the master. This is the logarithm to the base 2 of the delay request interval in seconds.
This value ranges between 0 and 5. |
| enable | - | Enables PTP in the domain. |

	sync	-	Logarithm to the base 2 of the sync message interval in seconds. Sync message is the event message used for slave clock synchronization and will be time stamped. This value ranges between -1 and 1.
	limit	-	Maximum clock offset value before which the PTP attempts to resynchronize. This value ranges between 50 and 1000000000 nanoseconds.
	delay mechanism	-	Propagation delay measuring option used by the port in computing the mean path delay. Options are: 1 – End-to-end delay measurement mechanism between slave clocks and the master clock. 2 – Peer-to-peer delay measurement mechanism between slave clocks and the master clock.
	version	-	PTP version on which the PTP receive time stamp configuration is applicable. Options are: 1 – PTP version 1. 2 – PTP version 2.
	domain	-	Unique identifier of the domain. This domain ID defines the scope of the PTP message communication, state, operations, data sets and timescale. This value ranges between 0 and 255.
		0	Default domain ID.
		1 to 3	Alternate domains.
		128 to 255	Reserved.
	ipv6	-	Internet Protocol version 6.
Mode	Interface Configuration Mode / VLAN Configuration Mode		
Package	Workgroup, Enterprise and Metro		
Defaults	announce	-	1
	timeout	-	3

delay-req interval	-	0
interval	-	0
limit	-	1000000000 nanoseconds
delay mechanism	-	1
version	-	2

Example `iss(config-if)# ptp sync interval 1 domain 2 ipv6`

**Related
Command**

- **show ptp port** - Displays all the PTP port properties of the given virtual switch and domain.
- **show ptp foreign-master-record** - displays the PTP foreign-master information of the given virtual switch and domain.
- **show ptp counters** - Displays all the PTP port counters of the given virtual switch and domain.

62.22 ptp alternate-master - ipv6

This command enables PTP alternate master option and configures alternate sync interval. The interval is set using log base 2 values. The no form of the command disables PTP alternate master option and resets the alternate sync interval to default values.

```
ptp alternate-master { alternate-multisync | multisync-interval <short (0-255)> } [domain <short (0-127)>] [ ipv6 ]
```

```
no ptp alternate-master { alternate-multisync | multisync-interval <short (0-255)> } [domain <short (0-127)>] [ ipv6 ]
```

Syntax Description	alternate-multisync	- This is TRUE and if the port is transmitting multicast announce message with alternate master flag true, then the slave port can also transmit multicast sync messages with alternate master flag as true
	multisync-interval	- Interval in seconds between the sync messages transmitted with alternate master flag as true. This value ranges between 0 and 255.
	domain	- Unique identifier of the domain. This domain ID defines the scope of the PTP message communication, state, operations, data sets and timescale. This value ranges between 0 and 255. 0 Default domain ID. 1 to 3 Alternate domains. 128 to 255 Reserved.
	ipv6	- Internet Protocol version 6.

Mode Interface Configuration Mode / VLAN Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults

alternate-multisync	-	false
multisync-interval	-	0

Example

```
iss(config-ptp)# ptp alternate-master alternate-multisync domain 2 ipv6
```

Related Command **show ptp port** - Displays all the PTP port properties of the given virtual switch and domain.

62.23 ptp acceptable-master enable - ipv6

This command enables acceptable master option on the port. The no form of the command disables acceptable master option on the port.

```
ptp acceptable-master enable [domain <short(0-127)>] [ ipv6 ]
```

```
no ptp acceptable-master enable [domain <short(0-127)>] [ ipv6 ]
```

Syntax Description	domain	-	Unique identifier of the domain. This domain ID defines the scope of the PTP message communication, state, operations, data sets and timescale. This value ranges between 0 and 255.	
			0	Default domain ID.
			1 to 3	Alternate domains.
			128 to 255	Reserved.
	ipv6	-	Internet Protocol version 6.	
Mode	Interface Configuration Mode / VLAN Configuration Mode			
Package	Workgroup, Enterprise and Metro			
Defaults	Acceptable master option is disabled.			
Example	iss(config-if)# ptp acceptable-master enable domain 2 ipv6			
Related Command	show ptp acceptable masters - Displays PTP acceptable master information of the given virtual switch and domain.			

62.24 ptp max alternate-masters - ipv6

This command configures the number of alternate masters on the port. The no form of this command resets the number of alternate masters on the port to default values.

```
ptp max alternate-masters <value(0-255)> [domain <short(0-127)>] [ ipv6 ]
```

```
no ptp max alternate-masters [<integer(0-255)>] [domain <short(0-127)>] [ ipv6 ]
```

Syntax Description	domain	- Unique identifier of the domain. This domain ID defines the scope of the PTP message communication, state, operations, data sets and timescale. This value ranges between 0 and 255.
		<div>0 Default domain ID.</div> <div>1 to 3 Alternate domains.</div> <div>128 to 255 Reserved.</div>
	ipv6	- Internet Protocol version 6.

Mode Interface Configuration Mode / VLAN Configuration Mode

Package Workgroup, Enterprise and Metro

Defaults Number of alternate masters is 0.

Example iss(config-if)# ptp max alternate-masters 10 domain 2 ipv6

Related Command **show ptp port** - Displays all the PTP port properties of the given virtual switch and domain.

62.25 show ptp global info

This command displays the PTP clock global information.

show ptp global info

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ptp global info

```
PTP System Status
-----
Global Status : Start
Primary Context : default
Enabled Notifications :
    - global error
    - system control
    - system admin change
    - port state change
    - port admin change
    - sync fault
    - grand master fault
    - acceptable master fault
```

Related Command **shutdown ptp** - Shuts down PTP in the device.

62.26 show ptp vrf | switch info

This command displays the PTP clock information for a context.

```
show ptp { vrf | switch } <context-name> info
```

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ptp vrf default info

```
PTP Context Information
-----
PTP Status      : Enabled
Primary Domain  : 0
Debug Status    : critical
```

Related Command

- **ptp - vrf | switch** - Creates a PTP domain in a virtual context.
- **ptp enable | disable** - Enables PTP in a virtual context.

62.27 show ptp clock

This command displays the PTP clock properties of the given virtual switch and domain. If the virtual context and domain is not specified, this command displays the PTP clock properties of the default context and default domain.

```
show ptp clock [{ vrf | switch } <context-name>] [domain <id (0-127)>]
```

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ptp clock switch sw2 domain 0

PTP Clock Information

```
-----
PTP Device Type           : Interface Masters PTP
Clock Identity            :
Clock Context             : sw2
Clock Domain              : 0
Primary Domain            : 0
```

```

Clock Mode                : Ordinary
Type Of Clock             : One Step
Number of PTP ports       : 1
Priority1                  : 128
Priority2                  : 128
```

```

Clock Quality
  Class                   : 248
  Accuracy                 : 254
  Offset (log variance)   : 0
```

```
Local Clock Time          : 0
```

- Related Command**
- **ptp primary-domain** - Configures the current domain as PTP primary domain which can configure the system clock.
 - **ptp two-step-clock** - Configures PTP clock as two step clock.
 - **ptp clock ports** - Configures the number of PTP clock ports on the device.
 - **ptp mode** - Configures PTP clock mode and clock priorities.
 - **ptp slave** - Configures the clock as a slave only clock.
 - **ptp pathtrace** - Enables PTP pathtrace option in the system.

62.28 show ptp foreign-master-record

This command displays the PTP foreign-master information of the given virtual switch and domain. If the virtual context and domain is not specified, this command displays the PTP foreign-master information of the default context and default domain.

```
show ptp foreign-master-record [{ vrf | switch } <context-name>] [domain <id
(0-127)>]
```

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ptp foreign-master-record

```
PTP Foreign Master Record
-----
      Foreign Master Identity
      Clock Identity          :
00:01:02:ff:fe:03:04:01
      Port Identity           : 1
      Number of announce messages : 9
```

Related Command

- **ptp** - Configures PTP system parameters.
- **ptp - ipv6** - Configures PTP system parameters.

62.29 show ptp parent

This command displays the parent and grand-master properties of the given virtual switch and domain. If the virtual context and domain is not specified, this command displays the parent and grand-master properties of the default context and default domain.

```
show ptp parent [{ vrf | switch } <context-name>] [domain <id (0-127)>]  
[stats]
```

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ptp parent

PTP Parent Properties

Parent Clock

Parent Clock Identity : 00:01:02:ff:fe:03:04:01

Parent Port Number : 1

Parent Offset (log variance) : 0

Parent Clock Phase Change Rate : 0

Grandmaster Clock

Grandmaster Clock Identity : 00:01:02:ff:fe:03:04:01

Grandmaster Clock Quality : 0

Class : 248

Accuracy : 254

Priority1 : 128

Priority2 : 128

Observed Drift : 0

Offset (log variance) : 0

Related Command **ptp mode** - Configures PTP clock mode and clock priorities.

62.30 show ptp port

This command displays all the PTP port properties of the given virtual switch and domain. If the virtual context and domain is not specified, this command displays all the PTP port properties of the default context and default domain.

```
show ptp port [{[ vrf | switch ] <string (32)>] | [{ ipv4 | ipv6 }] {<ifXtype>
<ifnum> | vlan <integer> [switch <string(32)>]}} [domain <short (0-127)>]
```

Syntax Description	vrf	-	Name of the VRF instance. This value is a string of size 32.
	switch	-	Name of the switch context. This value is a string of size 32.
	ipv4	-	Internet Protocol version 4.
	ipv6	-	Internet Protocol version 6.
	ifXtype	-	Ethernet interface type assigned in the interface manager of the system.
	ifnum	-	Ethernet interface index number assigned in the interface manager of the system.
	vlan	-	VLAN identifier assigned in the interface manager of the system.
	switch	-	32-bit unique context identifier. Each virtual context will be able to run PTP individually and this distinguishes multiple virtual contexts present in the switch/router. This value ranges between 0 and 255.
	domain	-	Unique identifier of the domain. This domain ID defines the scope of the PTP message communication, state, operations, data sets and timescale. This value ranges between 0 and 255.
		0	0
		1 to 3	1 to 3

	128 to 255	128 to 255
Mode	Privileged EXEC Mode	
Package	Workgroup, Enterprise and Metro	
Example	<pre> iss# show ptp port switch sw1 domain 0 PTP Port Properties ----- Record # 1 Device type : IEEE 802.3 Switch / Vrf : sw1 Interface : gigabitethernet 0/1 Port identity : 00:08:02:ff:fe:03:04:02 :0 PTP version : 2 Delay mechanism : Peer to Peer Sync Fault Limit : 50000 PTP Status : Enable PTP State : Master Alt Master : Enabled Alt SyncInterval : 10 Port Timers : Announce receipt Timeout : 2 Peer mean path delay : 0 Announce Interval : 2 Sync Interval : 1 Delay request Interval : 2 Peer delay request Interval : 0 </pre>	
Related Command	<ul style="list-style-type: none"> • ptp port - Adds port to the PTP clock. • ptp alternate-master - Enables PTP alternate master option and configures alternate sync interval. • ptp max alternate-masters - Configures the number of alternate masters on this port. • ptp - Configures PTP system parameters. • ptp - ipv6 - Configures PTP system parameters. • ptp alternate-master - ipv6 - Enables PTP alternate master option and configures alternate sync interval. 	

62.31 show ptp counters

This command displays all the PTP port counters of the given virtual switch and domain.

```
show ptp counters [{ vrf | switch } <context-name>][domain <id (0-127)>]
```

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ptp counters

PTP Interface Counters

```
Interface gigabitethernet 0/1
  Announce Messages Received : 38
  Sync Messages Received    : 75
  Delay Requests Received    : 0
  Delay Responses Received   : 75
  Delay Requests Transmitted : 0
  Discarded Messages        : 12
```

Related Command

- **ptp** - Configures PTP system parameters.
- **ptp - ipv6** - Configures PTP system parameters.

62.32 show ptp time-property

This command displays the PTP time properties of the given virtual switch and domain. If the virtual context and domain is not specified, this command displays the PTP time properties of the default context and default domain.

```
show ptp time-property [{ vrf | switch } <context-name>][domain <id(0-127)>]
```

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ptp time-property

```
PTP Clock Time Property
-----
Current UTC offset valid : 0
Current UTC offset      : 0
Leap 59                  : 0
Leap 61                  : 0
Time traceable           : 0
Frequency traceable      : 0
Time source               : 0
```

62.33 show ptp current

This command displays PTP current offset and meanpath delay value with the master of the given virtual switch and domain. If the virtual context and domain is not specified, this command displays PTP current offset and meanpath delay value with the master of the of the default context and default domain.

```
show ptp current [{ vrf | switch } <context-name>] [domain <id (0-127)>]
```

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ptp current

```
PTP Clock Current Information
-----
Current Steps Removed      : 1
Current Offset from Master : 0
Current Mean Path Delay    : 1966
```

Related Command **ptp alternate-time-scale key** - Configures PTP alternate time scale properties, current-offset, jump-seconds and next-jump in seconds.

62.34 show ptp acceptable masters

This command displays PTP acceptable master information of the given virtual switch and domain. If the virtual context and domain is not specified, this command displays PTP acceptable master information of the default context and default domain.

```
show ptp acceptable masters [{ vrf | switch } <context-name>] [domain <id (0-127)>]
```

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ptp acceptable masters switch sw2 domain 2

```
PTP Acceptable Masters
-----
Record # 1
    Protocol      :  UDP /IP Version 4
    Address       :  10.0.0.1
    AltPriority    :  50
Record # 2
    Protocol      :  UDP /IP Version 6
    Address       :  482f::4830
    AltPriority    :  50
Record # 3
    Protocol      :  Ethernet
    Address       :  00:80:30:ff:fe:10
    AltPriority    :  50
```

Related Command

- **ptp acceptable-master protocol** - Configures the PTP acceptable masters.
- **ptp acceptable-master enable** - Enables acceptable master option on port.

62.35 show ptp alternate time-scale

This command displays PTP alternate timescale properties of the given virtual switch and domain. If the virtual context and domain is not specified, this command displays PTP alternate timescale properties of the default context and default domain.

```
show ptp alternate time-scale [{ vrf | switch } <context-name>] [domain <id  
(0-127)>]>
```

Mode Privileged EXEC Mode

Package Workgroup, Enterprise and Metro

Example iss# show ptp alternate time-scale switch sw2 domain 2

PTP Alternate Time Scale

Record # 1

```
Alternate Time Scale Key Index      : 1
Alternate Time Scale offset         : 10
Alternate Time Scale jump Seconds   : 20
Alternate Time Scale Next jump      : 50
Alternate Time Scale Display Name   : NTP
```

- Related Command**
- **ptp alternate-time-scale key** - Configures the alternate time scale that PTP grandmaster supports.
 - **ptp alternate-time-scale enable key** - Enables PTP alternate time scale option.
 - **ptp alternate-time-scale key** - Configures PTP alternate time scale properties, current-offset, jump-seconds and next-jump in seconds.

62.36 debug ptp

This command enables global trace messages, if global option is selected and enables PTP trace messages on the given virtual switch and domain. The no form of the command disables global trace messages, if global option is selected and disables PTP trace messages on the given virtual switch and domain.

```
debug ptp { global | { vrf | switch } <string(32)> } { all | [init-shut]
[mgmt] [datapath] [ctrl] [pkt-dump] [resource] [all-fail] [buffer] [critical]
}
```

```
no debug ptp { global | { vrf | switch } <string(32)> } { all | [init-shut]
[mgmt] [datapath] [ctrl] [pkt-dump] [resource] [all-fail] [buffer] [critical]
}
```

Syntax Description	global	- Global trace option.
	vrf	- Name of the VRF instance. This value is a string of size 32.
	switch	- Name of the switch context. This value is a string of size 32.
	all	- All traces.
	init-shut	- Start and Shutdown traces.
	mgmt	- Management traces.
	datapath	- Data packet path.
	ctrl	- Control plane path.
	pkt-dump	- Packet Dump traces.
	resource	- Resource failure traces.
	all-fail	- All failure traces.
	buffer	- Buffer traces.
	critical	- PTP critical traces.

ISS

Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise and Metro
Defaults	critical
Example	<code>iss# debug ptp global init-shut pkt-dump buffer</code>

Chapter

63

Layer 4 Switching

Layer 4 switching refers to a product's ability to make various traffic handling decisions based on the contents of OSI layer 4 (the Transport Layer). A Layer 4 switch not only examines the IP address, but also controls the traffic based on the port numbers located at Layer 4 of the OSI model.

Layer 4 switching technology greatly enhances the intelligence of the network. High-speed hardware is used to implement the intelligent decision making capability of the Layer 4 switch, thus allowing high capacity networks to function very efficiently. Layer 4 switching enables application redirection. It is also used to enable prioritization of traffic based on specific applications.

Note: Layer 4 switching in **Interface Masters ISS** controls the traffic based on the port numbers and the protocols located at Layer 4 of the OSI model

The list of CLI commands for the configuration of Layer 4 Switching is as follows:

- layer4 switch
- show layer4 switch

63.1 layer4 switch

This command adds a Layer 4 Switching entry in to the table. The no form of the command deletes the Layer 4 Switch entry from the table.

```
layer4 switch <FilterNo (1-20)> protocol { any | tcp | udp | <Protocol No (1-255)>} port { any | <PortNo (1-65535)>} interface { <interface type> <interface id> }
```

```
no layer4 switch <FilterNo (1-20)>
```

Syntax Description	FilterNo	- Filter Number
	protocol	- Layer 4 Protocol, can be any tcp udp Protocol no
	port	- Port can be, any Portnumber
	interface	- Denotes packet to be switched to the given interface
Mode	Global Configuration Mode	
Example	<pre>iss(config)# layer4 switch 1 protocol any port 88 interface gigabitethernet 0/1</pre>	
Related Command	show layer4 switch – Displays the Layer 4 Switch entry in the table	

63.2 show layer4 switch

This command displays the Layer 4 Switch entry in the table.

```
show layer4 switch { all | <FilterNo (1-20)> }
```

Syntax Description	all	- All entries
	FilterNo	- Displays entries for the given filter number
Mode	Privileged/User EXEC Mode	
Example	iss# show layer4 switch all	
	<pre> Layer 4 Switching Filter ----- Protocol PortNo CopyToPort ----- TCP ANY 1 ANY 88 2 </pre>	
Related Command	layer4 switch - Adds a Layer 4 Switching entry in to the table	